FORMAT OF THE CERTIFICATE (VERSION 0.1)

J. FRANKE, T. KLEINJUNG, A. DECKER, A. GROSSWENDT

This document explains the format of the certificate produced by our implementation of a primality test along the lines proposed by Mihailescu [Mih06a] and [Mih06b]. It is intended to convince the reader that such certificates indeed prove the primality of the numbers for which they have been issued.

The certificate is a (possibly compressed) archive file containing a directory containing various data. Let n`.cert` be the name of the directory. The directory will always contain a file n`.ecpp`, the first non-empty line of which contains the decimal representation of the number whose primality is to be certified. The format of n`.ecpp` is an extension of the classical Atkin-Morain `ECPP` format which allows for the possibility to terminate the certificate by a Mihailescu twin rather than by a number which is small enough for trial division. This format, along with the format of the other files forming the primality proof, is described below.

The format of the certificate as an archived directory has been chosen because of the complex nature of the test, which makes it desirable to have easy ways to enable the use of improvements to the method. For instance, it seems likely that the use of methods for finding divisors in residue classes such as [CHGN08] (improving [Len84]) as described in remark 7 provides a considerable speed-up as well as shorter certificates.

The format of n`.ecpp` also provides the possibility of specifying a version number. This document describes version 0.1 of the certificate.

Contents

1. Goldwasser-Kilian-chains and Mihailescu twins

1.1. **Goldwasser-Kilian-chains.** All schemes are assumed to be Noetherian. The notion of an elliptic curve over a scheme will be understood as in [KM85]. An elliptic curve over a ring R is an elliptic curve over $\operatorname{Spec} R$.

A Goldwasser-Kilian (GK) chain link is a triple $(\mathcal{E}, P, q)$, where $\mathcal{E}$ is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, P a $\mathbb{Z}/N\mathbb{Z}$-valued point on it, and q an integer, such that P is disjoint[1] from the neutral element $\mathbb{O}$ of $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$, and such that

$$q \cdot P = \mathbb{O} \tag{1}$$

and

$$q > \sqrt{N} + 2\sqrt[4]{N} + 1. \tag{2}$$

In this situation, the primality of N may be derived from the primality of q, using Hasse's theorem about the group order of elliptic curves over finite fields.

While it should normally be possible to directly apply the Mihailescu primality test to an input number, it may sometimes be better to reduce the primality of the input number to the primality of a different number for which it is easier to find the Mihailescu twin required for the test. This is the reason for the presence of the file `n.ecpp` in the certificate, whose format will be described after introducing the notion of a Mihailescu twin.

1.2. **Mihailescu twins.** Let K be an imaginary quadratic field. The complex conjugate of an element x of a CM-field like K will normally be denoted $\overline{x}$. An elliptic curve with complex multiplication by $\mathcal{O}_K$ (where $\mathcal{O}_L$ denotes the ring of integers in a number field L) is an elliptic curve $\mathcal{E}$ over S together with a morphism $[\cdot]_{\mathcal{E}}$ from $\mathcal{O}_K$ to the ring of

[1] in the sense that its intersection with the zero point $\mathbb{O}$ is empty. In the usual settings of a Weierstraß cubic $y^2 = x^3 + ax + b$ with the neutral element $[1, 0, 0]$, this is the case if and only if the point P may be given by affine (x, y)-coordinates.

endomorphisms of $\mathcal{E}$. By the action of the complex multiplication on the tangent space at the neutral element, this turns S into a $\operatorname{Spec}\mathcal{O}_K$-scheme. If the dual f^t of an isogeny f is defined as in [KM85] and if S is connected, then for $x \in \mathcal{O}_K$ we have $[x]_{\mathcal{E}}^t = [x^t]_{\mathcal{E}}$ for some $x^t \in \mathcal{O}_K$ with $x + x^t \in \mathbb{Z}$, since by [KM85, Corollary 2.6.2.2] $[x_{\mathcal{E}}]^t + [x]_{\mathcal{E}}$ is multiplication by some integer. But the only suitable involution of $\mathcal{O}_K$ is $x^t = \overline{x}$. Applying this to the connected components of S shows that $[x]_{\mathcal{E}}^t = [\overline{x}]_{\mathcal{E}}$ for general S, and by [KM85, Theorem 2.6.1] it follows that the degree of $[x]_{\mathcal{E}}$ equals $N(x) = x \cdot \overline{x}$. The image of a point P under $[x]_{\mathcal{E}}$ will often be denoted $x \cdot P$.

Definition 1. A Mihailescu twin is a tuple $(K, E_1, E_2, \nu_1, \nu_2)$, where K is an imaginary quadratic number field, E_k an elliptic curve $\mathcal{E}_k$ over $\mathbb{Z}/N_k\mathbb{Z}$ with a point $P_k \in \mathcal{E}_k(\mathbb{Z}/N_k\mathbb{Z})$ on it and with complex multiplication by $\mathcal{O}_K$, and ν_k an element of $\mathcal{O}_K$ such that the following conditions hold:

- $N_{K/\mathbb{Q}}(\nu_k) = N_k$.
- $\mathbb{Z} \cap \nu_k\mathcal{O}_k = N_k\mathbb{Z}$, and the composition $\mathcal{O}_K \to \mathcal{O}_K/\nu_k$ with the inverse of the isomorphism $\mathbb{Z}/N_k\mathbb{Z} \to \mathcal{O}_K/\nu_k\mathcal{O}_K$ coincides with the homomorphism $\mathcal{O}_K \to \mathbb{Z}/N_k\mathbb{Z}$ defined by the complex multiplication on $\mathcal{E}_k$.
- The pair $\big((\mathcal{E}_k, P_k), N_{3-k}\big)$ is a valid Goldwasser-Kilian chain link reducing the primality of N_k to the primality of N_{3-k}.
- We have

$$\nu_{3-k} \cdot P_k = 0 \tag{3}$$

  in $\mathcal{E}_k(\mathbb{Z}/N\mathbb{Z})$.
- $\nu_1 + \nu_2 = 1$.
- N_1N_2 is odd.

Remark 1. Because of the third of the above conditions, the numbers N_1 and N_2 are either both primes or both composites. Note that we have $|N_k - N_{3-k} + 1| \leq 2\sqrt{N_k}$ by the first and fifth conditions such that (2) in the third condition is trivial if $\min(N_1, N_2) > 16$.

Remark 2. Note that our conditions imply $D \equiv 5 \pmod 8$ for the discriminant D of K since otherwise one of N_1 or N_2 must be even.

Throughout the rest of this subsection, let $(K, E_1, E_2, \nu_1, \nu_2)$ be a Mihailescu twin, and let $\mathcal{E}_k$, P_k, N_k, and D be the same as before.

In the following considerations, k will always be assumed to be $\in \{1; 2\}$. If r is a prime divisor or N_k, $\mathcal{E}_k\,|_r$ denotes the fiber product $\mathcal{E}_k \bigtimes_{\operatorname{Spec}(\mathbb{Z}/N\mathbb{Z})} \operatorname{Spec}(\mathbb{F}_r)$, together with the similar base change of the complex multiplication, and $P_k\,|_r$ will denote the morphism

$\operatorname{Spec}(\mathbb{F}_r) \xrightarrow{(P_k j, \operatorname{Id}_{\operatorname{Spec}(\mathbb{F}_r)})} \mathcal{E}_k \bigtimes_{\operatorname{Spec}(\mathbb{Z}/N\mathbb{Z})} \operatorname{Spec}(\mathbb{F}_r)$, where j is the unique morphism $\operatorname{Spec}(\mathbb{F}_r) \xrightarrow{j} \operatorname{Spec}(\mathbb{Z}/N\mathbb{Z})$. Moreover, let $E_k\,|_r$ be the pair $(\mathcal{E}_k\,|_r\,, P_k\,|_r)$.

If r is prime and X a $\mathbb{F}_r$-scheme, let the absolute Frobenius $\mathfrak{F}_X$ be the endomorphism of X which acts as the identity on points and with $\mathfrak{F}_X^* f = f^r$ for any section of the structure sheaf. If follows that $F_Y \xi = \xi F_X$ for any morphism $X \xrightarrow{\xi} Y$ of $\mathbb{F}_r$-schemes.

If $\mathcal{E}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ over any field and ϕ an endomorphism of $\mathcal{E}$ which commutes with the complex multiplication, then $\phi = [f]_{\mathcal{E}}$ for a uniquely determined element f of $\mathcal{O}_K$. This follows from the fact that, by [Hus04, Theorem 12.4.6, Proposition 13.6.2, Theorem 13.6.3] and since $\mathcal{O}_K$ is integrally closed in K, $[\mathcal{O}_K]_{\mathcal{E}}$ is the maximal commutative subring of $\operatorname{End}(\mathcal{E})$ containing $[\mathcal{O}_K]_{\mathcal{E}}$. If $\mathcal{E}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ over $\mathbb{Z}/N\mathbb{Z}$ and r a prime divisor of N, then this may be applied to $\phi = \mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r}$ and shows that there is a unique element $\pi_r^{(\mathcal{E})} \in \mathcal{O}_K$ such that $\mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r} = [\pi_r^{(\mathcal{E})}]_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r}$. This is a prime element dividing r since its norm is equal to the degree of $\mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r}$ which is r. Obviously, $\pi_r^{(\overline{\mathcal{E}})} = \overline{\pi_r^{(\mathcal{E})}}$. The prime ideal $\mathfrak{p}_r^{(\mathcal{E})}$ generated by $\pi_r^{(\mathcal{E})}$ is the preimage of $r\mathbb{Z}/N\mathbb{Z}$ under the homomorphism $\mathcal{O}_K \to \mathbb{Z}/N\mathbb{Z}$ defined by the way in which the complex multiplication on $\mathcal{E}$ acts on the tangent space of $\mathcal{E}$ at 0. This is so because that preimage must contain $\mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r}$, which acts as 0 on the tangent space. The relative (with respect to $\operatorname{Spec}\mathbb{F}_r$) Frobenius on $\mathcal{E}\times\operatorname{Spec}\overline{\mathbb{F}_r}$ is also given by $\pi_r^{(\mathcal{E})}$ since

$$\begin{aligned}\mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\overline{\mathbb{F}_r}} &= \mathfrak{F}_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r} \times \mathfrak{F}_{\operatorname{Spec}\overline{\mathbb{F}_r}} = \\ &= [\pi_r^{(\mathcal{E})}]_{\mathcal{E}\times\operatorname{Spec}\mathbb{F}_r} \times \mathfrak{F}_{\operatorname{Spec}\overline{\mathbb{F}_r}} = [\pi_r^{(\mathcal{E})}]_{\mathcal{E}\times\operatorname{Spec}\overline{\mathbb{F}_r}} \circ \big(\operatorname{Id}_{\mathcal{E}} \times \mathfrak{F}_{\operatorname{Spec}\mathbb{F}_r}\big),\end{aligned}$$

and it follows from the proof of [KM85, Corollary 2.6.4] or of [Hus04, Theorem 13.1.2] that the number of $\mathbb{F}_r$-valued points on $\mathcal{E}$ equals

$$\#\big(\mathcal{E}(\mathbb{F}_r)\big) = N(1 - \pi_r^{(\mathcal{E})}).$$

If no ambiguity exists, we will use the shortcuts π_r and $\mathfrak{p}_r$. In particular, $\pi_r = \pi_r^{(\mathcal{E}_k)}$ if r divides N_k.

Let b be the smallest prime divisor of $N_1 N_2$.

Lemma 1. *If r is a prime divisor of N_k and the group order $r' = N_{K/\mathbb{Q}}(1 - \pi_r)$ of $\mathcal{E}_k\,|_r$ is $< 2b$, then r' is a prime divisor of N_{3-k}.*

Proof. Indeed, the point $P_k\,|_r$ is not zero, since P_k was assumed to be disjoint from zero. The order o of $P_k\,|_r$ in $\mathcal{E}_k\,|_r\,(\mathbb{F}_r)$ is a divisor of

N_{3-k}, as $N_{3-k}P_k = 0$. If o was less than the full group order r', it would be $< b$, contradicting the minimality of b. If r' was composite, it would have to have prime divisors $\leq r'/2 < b$ also contraticting the minimality of b. □

Theorem 1. *Let $D < -3$, and let p be the smallest prime number which splits into more than one prime factor in $\mathcal{O}_K$. Assume that b is so large that*

$$(\sqrt{b} + p - 1)^2 < 2b. \tag{4}$$

Then there exist prime divisors r_1 of N_1 and r_2 of N_2 such that the tuple

$$(K, E_1\,|_{r_1}\,, E_2\,|_{r_2}\,, \pi_{r_1}, \pi_{r_2}) \tag{5}$$

is a Mihailescu twin. Moreover, the numbers r_1 and r_2 can be chosen such that they are both $\leq (\sqrt{b} + p - 2)^2$.

Proof. We assume that this is not the case and derive a contradiction. Since the situation is symmetric, we may without losing generality assume that b divides N_1. Let $\beta = \pi_b$. To derive a contradiction, we prove

(+) If $k < p$, then $r_k = N(\beta - k)$ is a prime divisor of N_1 for even and of N_2 for odd k. Moreover, if $k < p - 1$ then π_{r_k} equals $\beta - k$.

By our assumption on p, the residue field of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ above p is $\mathbb{F}_p$. Therefore, one of the elements $\beta, \beta - 1, \ldots, \beta + 1 - p$ must be $\in \mathfrak{p}$. Thus, one of the numbers r_k with $0 \leq k < p$ must be be divisible by p. But it is a prime divisor of $N_1 N_2$ and therefore equal to p and $\geq b$, contradicting (4).

To show (+), we use induction on k. If $k = 0$, (+) follows from the definition of b and β and the choice of an order of the two components of the twin. Let us assume $k > 0$ and that (+) holds with k replaced by $k - 1$. Let $j = 1$ for even and $j = 2$ for odd k, then r_{k-1} is a prime divisor of N_{3-j} and $\pi_{r_{k-1}}$ equals $\beta + 1 - k$, such that the group order of $\mathcal{E}_{3-j}(\mathbb{F}_{r_{k-1}})$ equals $N_{K/\mathbb{Q}}\big(1 - (\beta + 1 - k)\big) = N_{K/\mathbb{Q}}(\beta - k)$. Since $k < p$ and $\sqrt{r_k} \leq \sqrt{b} + k$, we have $r_k < 2b$. We are thus able to apply lemma 1 and conclude that r_k is a prime divisor of N_j.

It follows that $1 - (\beta + 1 - k) = k - \beta$ is a prime element. Moreover, this prime element divides μ_j. This is so because $P_{3-j}\,|_{r_{k-1}}$ is invariant under the relative Frobenius $F_{r_{k-1}}$, which equals $\pi_{r_{k-1}} = \beta + 1 - k$. Therefore,

$$(\beta + 1 - k) P_{3-j}\,|_{r_{k-1}} = P_{3-j}\,|_{r_{k-1}}$$

or $(\beta - k)P_{3-j}\,|_{r_{k-1}} = 0$ in $\mathcal{E}_{3-j}(\mathbb{F}_{r_{k-1}})$. But $\mu_j P_{3-j}\,|_{r_{k-1}} = 0$ since one of our assumptions on Mihailescu twins is $\mu_j P_{3-j} = 0$. Since $\beta - k$ is a prime element and since $P_{3-j}\,|_{r_{k-1}} \neq 0$, $\beta - k$ must divide μ_j as stated.

As the structure of an $\mathcal{O}_K$-algebra on $\mathbb{Z}/N_j\mathbb{Z}$ defined by the complex multiplication on $\mathcal{E}_j$ is given by $\mathcal{O}_K \to \mathcal{O}_K/\mu_j\mathcal{O}_K$ followed by the unique isomorphism $\mathcal{O}_K/\mu_j\mathcal{O}_K \to \mathbb{Z}/N_j\mathbb{Z}$, the ideal $\mathfrak{p}_{r_k}$ must be the ideal generated by $\beta - k$. Since $\mathcal{O}_K^\times = \{\pm 1\}$, the only generators of this ideal are $\beta - k$ and $k - \beta$. If $\pi_{r_k} = k - \beta$, then $(K, \mathcal{E}_j\,|_{r_k}, \mathcal{E}_{3-j}\,|_{r_{k-1}}, \pi_{r_k}, \pi_{r_{k-1}})$ is a Mihailescu twin with the desired properties, contradicting our assumption that the theorem is wrong. This leaves us with the choice $\beta - k$ for π_{r_k}, as in (+). □

While the specification of the number field K, the elements ν_k of $\mathcal{O}_K$, of the elliptic curves $\mathcal{E}_k$ and the points $P_k \in \mathcal{E}_k(\mathbb{Z}/N_k\mathbb{Z})$ is straightforward, the specification of complex multiplication requires some consideration. The complex multiplication may be specified by specifying the action of $\frac{a+\sqrt{-D}}{2}$ on $\mathcal{E}_k$, for some odd integer a. Since D tends to be so large (e. g., $D = 12238212163$ for the first 30000 digit number certified by the method) that direct specification or calculation with isogenies of degree $> \frac{D}{4}$ is not practical, one choses a in such a way that $\frac{a^2+D}{4}$ decomposes into sufficiently small prime factors. The action of $\frac{a+\sqrt{-D}}{4}$ on the curve is then not specified directly but by a chain of isogenies of smaller degree which are specified as will be explained below. The fact that these data indeed define complex multiplication on the curve may then be derived by using the following proposition.

Proposition 1. *Let N and D be natural numbers such that $-D$ is an odd fundamental discriminant, $K = \mathbb{Q}(\sqrt{-D})$, $\mathcal{E}$ an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, $\mathcal{E} \xrightarrow{\epsilon} \mathcal{E}$ an endomorphism of $\mathcal{E}$ and a an odd integer. Let $\mathfrak{n}$ be an ideal of $\mathcal{O}_K$ containing N and such that $\mathbb{Z}/N\mathbb{Z} \to \mathcal{O}_k/\mathfrak{n}$ is an isomorphism, and let $\lambda \in \mathbb{Z}/N\mathbb{Z}$ be the preimage under this isomorphism of the image of $\frac{a+\sqrt{-D}}{2}$ in $\mathcal{O}_k/\mathfrak{n}$. We assume that the degree d of ϵ equals $\frac{a^2+D}{4}$ and is coprime to n, that the endomorphism of the tangent space of $\mathcal{E}$ at its neutral element $\mathbb{O}$ defined by ϵ equals λ, and that N has no prime divisors $< 4\sqrt{d}$.*

Then there is a unique structure of complex multiplication by $\mathcal{O}_K$ on $\mathcal{E}$ such that $[\alpha]_{\mathcal{E}} = \epsilon$, where $\alpha = \frac{a+\sqrt{-D}}{2}$. Moreover, the action of $x \in \mathcal{O}_K$ on the tangent space of $\mathcal{E}$ at $\mathbb{O}$ defined by this structure of complex multiplication equals multiplication by the image of x in $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof. Over any connected component of $\operatorname{Spec}\mathbb{Z}/N\mathbb{Z}$, we have $\epsilon+\epsilon^t = [\operatorname{Tr}(\epsilon)]_{\mathcal{E}}$. We consider the action of these isogenies on the tangent space of $\mathcal{E}$ at $\mathbb{O}$ over this component. Let r be the prime divisor of N corresponding to the connected component, and let $\mathfrak{r}$ be the unique common prime divisor of $\mathfrak{n}$ and r in $\mathcal{O}_K$.

By our assumption on ϵ, the action of ϵ on the tangent space is given by $\alpha \bmod \mathfrak{r}$. Since $\epsilon\epsilon^t = [d]_{\mathcal{E}}$ ([KM85, Theorem 2.6.1]) the action of ϵ^t is given by $d/\alpha = \overline{\alpha}$ modulo $\mathfrak{r}$, and it follows that $\operatorname{Tr}(\epsilon) \equiv \operatorname{Tr}(\alpha) \pmod r$. We have $r > 4\sqrt{d}$ because of our assumption and since $4\sqrt{d}$ cannot be a prime divisor of N. Since $|\operatorname{Tr}(\alpha)| \leq 2\,|\alpha| = 2\sqrt{d}$ and since $\operatorname{Tr}(\epsilon) \leq 2\sqrt{d}$ ([KM85, Theorem 2.6.3]), it follows that $\operatorname{Tr}(\epsilon) = \operatorname{Tr}(\alpha)$ on the connected component under consideration, and again by [KM85, Theorem 2.6.3] that ϵ satisfies the equation $\epsilon^2 - \operatorname{Tr}(\alpha)\cdot\epsilon + d = 0$ satisfied by α. Since this holds over every connected component of $\operatorname{Spec}\mathbb{Z}/N\mathbb{Z}$, ϵ defines complex multiplication by $\mathcal{O}_K$.

The assertion about the action of $[x]_{\mathcal{E}}$ on the tangent space follows since it holds for $x = \alpha$ and when $x \in \mathbb{Z}$, and since α and 1 generate $\mathcal{O}_K$ as an abelian group. □

1.3. **Format of** n`.ecpp`**.** As was said before, the file format is an extension of the classical Atkin-Morain format to allow for the possibility of finishing the certificate by specifying a Mihailescu twin and some additional data.

The file is a sequence of blocks $B_1 \dots B_n$ separated by blank lines. Each block B_i starts with a line containing a integer $N = N_i$, followed either by a line containing the string `twin` followed by white space followed by a file name *tn* containing the name of a file specifying (part of) a Mihailescu twin, or a line containing a positive integer D. In the first case, the line containing the twin file name terminates the file *n.ecpp* safe for an optional line containing the string `version` followed by spaces followed by a version number. In the second case, the line containing D must be followed by lines containing a positive integer h, followed by a positive integer o, followed by positive integers $p_1, \dots, p_k$ followed by a line containing the integer 0, followed by lines containing positive integers a, b, x, y and q, followed by a line containing the integer 0. All numbers are given by their decimal representation.

To verify the validity of a block containing classical Atkin-Morain data (i. e., not terminated by a line starting with `twin`), one checks that $Y^2 = X^3 + aX + b$ defines an elliptic curve $\mathcal{E}$ over $\mathbb{Z}/N\mathbb{Z}$, that the point $P_o = (x, y)$ is on the curve, that $o = fq$ with $f = \prod_{j=1}^{k} p_j$, that $P = f \cdot P_o$ is disjoint from $\mathbb{O}$, and that $(\mathcal{E}, P, q)$ is a valid Goldwasser-Kilian chain link as defined near (1). For the numbers D and h, only

their positivity should be checked. Programs which create certificates and employ a version of the classical Atkin-Morain procedure (which currently seems to be the only competitive practical method for constructing Golwasser-Kilian chains starting from a generic input prime) should however set D such that $\mathcal{E}$ has complex multiplication by an order in $K = \mathbb{Q}(\sqrt{-D})$ and set h equal to the class number of K. Once the validity of the block B_i is checked, the primality of N_i follows from the primality of $q = q_i$.

The file n`.ecpp` is valid if all the blocks $B_1, \ldots, B_{n-1}$ are valid classical blocks reducing the primality of N_i to the primality of q_i, if $N_{i+1} = q_i$ for $1 \leq i < n$, and if either B_n is a valid classical block reducing the primality of N_n to the primality of q_n, or if B_n contains a line starting with `twin` specifying a Mihailescu twin for N_n. In the first case, the primality of N_1 must be proved by proving the primality of q_n by other means (eg, trial division). In the second case, the primality of the integer components of the twin must be checked as explained below in subsections 1.4, 2.4, 2.5, and 3.2.

1.4. **Format of the files specifying the Mihailescu twin.** The twin components N_1 and N_2 (integers), K (an imaginary quadratic number field) and $\nu_{1,2}$ (elements of $\mathcal{O}_K$) are specified in a file named *tn*. It is this file which, if a twin is present in the certificate, must be named on a line starting with `twin` in n`.ecpp`.

The file *tn* must contain a line containing the letter 'N' followed by a positive integer N_1, followed by a line containing the letter 'D' followed by a positive integer D, followed by a line containing 'X' followed by an integer x, followed by a line starting with 'Y' followed by an integer y, followed by a line containing the letter 'T' followed by a positive integer N_2. All integers are given in decimal representation.

Let $K = \mathbb{Q}(\sqrt{-D})$, $\nu_1 = \frac{x+y\sqrt{-D}}{2}$, $\nu_2 = 1 - \nu_1$. To check the validity of the file `tn`, verify that N_1 and N_2 are odd, that $-D$ is a fundamental discriminant, and that x and y are both odd. Moreover, check that at least one of the numbers N_1 or N_2 is equal to the number terminating the Goldwasser-Kilian chain in n`.ecpp`. Then, check that $N_i = N_{K/\mathbb{Q}}(\nu_i)$ and that y is coprime to N_1 and N_2. This also implies that x is coprime to N_1 and $2 - x$ to N_2, and ensures that $\mathcal{O}_K/\nu_i\mathcal{O}_K \cong \mathbb{Z}/N_i\mathbb{Z}$.

In the following, when we state that a piece of input text contains a residue class modulo a positive integer N, it is always assumed that it contains the decimal representation of the smallest non-negative representative of that residue class. Integers are also assumed to be given in their decimal representation.

The elliptic curves $\mathcal{E}_k$ with their points P_k are specified in files *tn.c*.`curve0`. Their complex multiplication is specified in *tn.c*.`CMdat`. The letter c is 'A' for $k = 1$ and 'B' for $k = 2$. If one of the numbers N_k is < 17, its primality will be decided by table lookup or trial division. Otherwise, an elliptic curve modulo N_k must be specified as follows.

The file *tn.c*.`curve0` contains four lines, each starting (in alphabetic order) with 'A', 'B', 'X' and 'Y', with the initial characters followed by residue classes a_k, b_k, ξ_k and υ_k modulo N_k. To confirm its validity, verify that $Y^2 = X^3 + a_k X + b_k$ defines an elliptic curve $\mathcal{E}_k$ over $\mathbb{Z}/N_k\mathbb{Z}$, that $P_k = (\xi_k, \upsilon_k)$ is a point of $\mathcal{E}_k$, and that $N_{3-k} \cdot P_k = \mathbb{O}$. Since we assume $N_k > 16$, it is then established by remark 1 that $(\mathcal{E}_k, P_k, N_{3-k})$ is a valid Goldwasser-Kilian chain link reducing the primality of N_k to that of N_{3-k}.

If at least one of the integer twin components is < 17, we have a valid Goldwasser-Kilian chain deducing the primality of the first number listed in *n*.`ecpp` from the primality of a number < 17. Otherwise, the primality of the integer twin components N_1 and N_2 will be confirmed by a method explained in the following subsections. This assumes that the curves $\mathcal{E}_k$ have complex multiplication by $\mathcal{O}_k$, and that theorem 1 is applicable.

To motivate the format of the files specifying complex multiplication, recall that for an elliptic curve $Y^2 = X^3 + AX + B$ over a field of characteristic > 3, $\frac{Y}{X}$ and $\frac{X^2}{Y}$ are formal parameters at $\mathbb{O}$ which define the same generator $g_{A,B}$ of the tangent space at $\mathbb{O}$. Recall from, e. g., [ABS08, Proposition 4.1] that under the previous assumptions, an isogeny of odd prime degree ℓ from an elliptic curve $\mathcal{E}$ given by $Y^2 = X^3 + AX + B$ to an elliptic curve $\tilde{E}$ given by $Y^2 = X^3 + \tilde{A}X + \tilde{B}$ which maps $g_{A,B}$ to $g_{\tilde{A},\tilde{B}}$ may be described as

$$(x, y) \longrightarrow \Big(\frac{\mathcal{N}(x)}{\mathcal{D}(x)}, y\big(\frac{\mathcal{N}}{\mathcal{D}}\big)'(x)\Big)$$

with $\mathcal{D} = g^2$, for a normed polynomial g of degree $\frac{\ell-1}{2}$, where

$$\frac{\mathcal{N}}{\mathcal{D}}(x) = \ell x - \sigma - \big(3x^2 + A\big)\frac{\mathcal{D}'}{\mathcal{D}}(x) - 2\big(x^3 + Ax + B\big)\Big(\frac{\mathcal{D}'}{\mathcal{D}}\Big)'(x) \tag{6}$$

with σ equal to the sum of zeros of the polynomial $\mathcal{D}(T)$, i. e., to $-2g_{\frac{\ell-3}{2}}$ if $g = \sum_{k=0}^{\frac{\ell-1}{2}} g_k T^k$. If the isogeny instead maps $g_{A,B}$ to $c g_{\tilde{A},\tilde{B}}$, with $c \neq 0$, it is instead given by

$$(x, y) \longrightarrow \Big(c^2\frac{\mathcal{N}(x)}{\mathcal{D}(x)}, c^3 y\big(\frac{\mathcal{N}}{\mathcal{D}}\big)'(x)\Big)$$

To test that this defines an isogeny, verify

$$c^6\mathcal{N}^3\mathcal{D} + c^2\tilde{A}\mathcal{N}^3\mathcal{D} + \tilde{B}\mathcal{D}^4 = c^6\big(T^3 + AT + B\big)\big(\mathcal{D}'\mathcal{N} - \mathcal{N}'\mathcal{D}\big)^2 \tag{7}$$

in the polynomial ring. These formulas may be used to specify isogenies over an arbitrary base ring R provided that it may be verified that $\mathcal{N}$ and $\mathcal{D}$ (or, equivalently, $\mathcal{N}$ and g) generate $R[T]$ as an ideal in $R[T]$, because in the language of schemes the isogeny may then be given by the triple

$$\Big[c^2\mathcal{N}(x)g(x), c^3y\big(\mathcal{N}'(x)g(x) - 2\mathcal{N}(x)g'(x)\big), g(x)^3\Big]$$

of elements of $\mathcal{O}_{\mathcal{E}}(-3\ell\mathbb{O}) \subseteq \mathcal{O}_{\mathcal{E}}\big(\mathcal{E}\setminus\mathbb{O}\big)$. When considered as sections of $\mathcal{O}_{\mathcal{E}}(-3\ell\mathbb{O})$ they have no common zeros, defining a morphism $\mathcal{E} \to \mathbb{P}^3_R$ which factors over $\tilde{\mathcal{E}} \subseteq \mathbb{P}^3_R$.

The format of the file *tn.c*`.CMdat` specifying the complex multiplication for $\mathcal{E}_k$ (with c equal to 'A' for $k = 1$ and 'B' for $k = 2$) is as follows. The first line starts with the letter 'A' followed by a positive integer a. The second line starts with the letter 'l' followed by a residue class λ modulo N_k. The third line starts with the letter 'N' followed by a positive integer n. These lines are followed by n blocks specifying n isogenies between elliptic curves. The j-th block starts with a line constisting of the letter 'D' followed by a positive integer ℓ_j. This is followed by a line starting with the two letters 'A' and 'B', followed by two residue classes α_j and β_j modulo N_k, which are separated by a space. This is followed by the coefficients $g_{j,i}$ of a normed polynomial $g_j(T) = \sum_{i=0}^{\frac{\ell-1}{2}} g_{j,i}T^i$. These are on separate lines given in order of increasing i with the line containing the i-th coefficient starting with the letter 'g', followed by the decimal representation of i, followed after a separating whitespace by the residue class $g_{j,i}$. We let j run from 0 to $n-1$.

To test the validity of *tn.c*`.CMdat`, verify that $\alpha_0 = a_k$ and $\beta_0 = b_k$. In other words, the (A,B)-pair of the curve starting the isogeny chain must coincide with the (A,B)-pair of the elliptic curve given in *tn.c*`.curve0`. Moreover, put $\alpha_n = \alpha_0$ and $\beta_n = \beta_0$, and let $\mathcal{F}_j$ be the elliptic curve over $\mathbb{Z}/N_k\mathbb{Z}$ given by $Y^2 = X^3 + \alpha_j X + \beta_j$. Verify that a is an odd integer, that $\frac{a^2+D}{4} = \prod_{j=0}^{n-1}\ell_j$, and that λ equals the image of $\frac{a+\sqrt{-D}}{2}$ in $\mathcal{O}_K/\nu_k\mathcal{O}_k \cong \mathbb{Z}/N_k\mathbb{Z}$. For $0 \le j < n$, verify that that g_j is a normed polynomial which by (6) defines an isogeny from $\mathcal{F}_j$ to $\mathcal{F}_{j+1}$ which maps g_{α_j,β_j} to $cg_{\alpha_{j+1},\beta_{j+1}}$ with $c = 1$ when $j \ne n-1$ and $c = \lambda$ if $j = n-1$. Recall that to verify that a normed polynomial g defines such an isogeny, one puts $\mathcal{D} = g^2$ and obtains $\mathcal{N}$ by (6), checks that g

and N generate the polynomial ring $\mathbb{Z}/N_k\mathbb{Z}[T]$ as an ideal, and verifies (7). Moreover, verify that N_k has no prime divisors $< 2\sqrt{a^2+D}$ and is coprime to all the ℓ_j (or, equivalently, that it is coprime to $\frac{a^2+D}{4}$). Once this is done, it follows from proposition 1 that the composition of the isogeny chain

$$\mathcal{E}_k = \mathcal{F}_0 \to \mathcal{F}_1 \to \ldots \mathcal{F}_n = \mathcal{E}_k \tag{8}$$

specified in the file defines, by giving the action of $\frac{a+\sqrt{-D}}{2}$, complex multiplication on $\mathcal{E}_k$ with an element of $\mathcal{O}_K$ acting trivially on the tangent space if it is divisible by ν_k.

It is now possible to verify (3). To do so, let $\alpha_k \in \mathbb{Z}$ be a representative of the image of $\frac{a+\sqrt{-D}}{2}$ under the projections

$$\mathcal{O}_K \to \mathcal{O}_K/\nu_{3-k}\mathcal{O}_K \cong \mathbb{Z}/N_{3-k}\mathbb{Z}.$$

In view of $N_{3-k} \cdot P_k = 0$, (3) can be checked by verifying that the result of applying the isogeny chain (8) to P_k equals $\alpha_k \cdot P_k$.

If all these validation steps terminate successfully and without an early confirmation of primality by the occurence of a prime < 16 in the Goldwasser-Kilian chain, it is confirmed that

$$\big(K, (\mathcal{E}_1, P_1), (\mathcal{E}_2, P_2), \nu_1, \nu_2\big) \tag{9}$$

is a Mihailescu twin, where $\mathcal{E}_k$ now is an elliptic curve over $\mathbb{Z}/N_k\mathbb{Z}$ with complex multiplication by $\mathcal{O}_K$, with coefficients a_k and b_k as above, and with the complex multiplication given in the files *tn.c*`.CMdat` as above. For the proof of primality, it will be necessary to confirm that theorem 1 may be applied. To do so, check that $D \neq -3$, and let p be the smallest prime number modulo which $-D$ is a square, and let

$$B = (1+\sqrt{2})(p-1). \tag{10}$$

Check that all prime divisors of N_1N_2 are $> B^2$. It is now clear that theorem 1 may be applied to (9).

2. Cyclotomic data

2.1. **FCE extensions.**

Definition 2. Let R be a commutative ring. By a free cyclic étale (FCE) extension of degree d of R we understand a pair (S, F), where S is an R-algebra which as an R-module is isorphic to R^d and F is an automorphism of S as an R-algebra such that $F^d = \mathrm{Id}_S$ and for each prime ideal $\mathfrak{p}$ of R and each algebraic closure $\overline{\mathfrak{k}}$ of its residue field, F acts transitively on the set $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \overline{\mathfrak{k}})$ of $\overline{\mathfrak{k}}$-valued points of the $\operatorname{Spec} R$-scheme $\operatorname{Spec} S$.

A morphism $(S, F) \to (\tilde{S}, \tilde{F})$ of FCE-algebras is a morphism

$$(S, F) \xrightarrow{\alpha} (\tilde{S}, \tilde{F})$$

of R-algebras satisfying $\alpha F = \tilde{F}\alpha$. It is an isomorphism if it is bijective.

By [GD67, Corollaire 17.6.2], an algebra R over a (Noetherian) ring S which is finitely generated and free of rank d as an R-module is étale if and only if for each maximal ideal $\mathfrak{m}$ of R, the R-algebra $S/\mathfrak{m}S$ decomposes as the set-theoretic product of separable field extensions of $R/\mathfrak{m}$. Since we have an epimorphism $S/\mathfrak{m}S \to \prod_{i=1}^{n} \mathfrak{k}_i$ where the $\mathfrak{k}_i$ are the residue fields of the prime ideals above $\mathfrak{m}$, this is the case if and only if the $\mathfrak{k}_i/\mathfrak{k}$ are separable and the sum of their degrees is d. Since the number of $\mathfrak{k}$-homomorphisms from $\mathfrak{k}_i$ to an algebraic closure $\bar{\mathfrak{k}}$ is $\leq [\mathfrak{k}_i : \mathfrak{k}]$ with equality if and only if the extension is separable, we see that S/R is étale if and only if $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ has precisely d elements, while it has less than d elements otherwise.

Lemma 2. *If S is an R-algebra which as an R-module is free of rank d and if F is an endomorphism of S such that $F^d = \mathrm{Id}_S$, then the following conditions are equivalent:*

- *(S, F) is an FCE-extension of R.*
- *For every prime ideal $\mathfrak{p}$ of R, any algebraic closure $\bar{\mathfrak{k}}$ of its residue field and any divisor $e < d$ of d, $\operatorname{Spec} F^e$ acts without fixed point on the set of $\bar{\mathfrak{k}}$-valued points of $\operatorname{Spec} S$.*
- *By F, S is a principal homogeneous space for the cyclic group $\mathbb{Z}/d\mathbb{Z}$ in the sense that*

$$S \otimes_R S \to S^d \qquad (11)$$

$$s_1 \otimes s_2 \to \big(s_1 \cdot F^i(s_2)\big)_{i=1}^{d}$$

is an isomorphism.

Proof. If the first condition holds, then in the situation of the second condition there are precisely d elements of $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ since S/R is étale, and F transitively acts on this set. It thus acts as a cyclic permutation of order d, and no smaller power of it has a fixed point. The second condition follows.

If the second condition holds and if $\mathfrak{p}$ and $\bar{\mathfrak{k}}$ are as in that condition, then $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ is not empty since S is a free R-module of finite rank $d > 0$. Because of the second condition, $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ cannot have less than d elements. In view of the above remark, S/R is étale. Moreover, every orbit of $\operatorname{Spec} F$ on $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ has d elements since no smaller power of $\operatorname{Spec} F$ has a fixed point. Thus, it acts transitively as required by the definition of FCE.

Geometrically, the third condition may be reformulated as saying that

$$(+) \qquad [\mathbb{Z}/d\mathbb{Z}] \times \operatorname{Spec} S \to \operatorname{Spec} S \underset{\operatorname{Spec} R}{\times} \operatorname{Spec} S$$
$$(n, s) \to (s, F^n S)$$

is an isomorphism, where the product on the left hand side is to be understood as the disjoint union of d copies of $\operatorname{Spec} S$. This implies the first condition as follows: Étaleness may be verified after the faithfully flat base change by $\operatorname{Spec} S \to \operatorname{Spec} R$ [GD67, Proposition 17.7.1], when it follows from the fact that the projection from the left hand side of $(+)$ to $\operatorname{Spec} S$ is clearly étale. Transitivity of the "Frobenius"-action on geometric fibres may also be verified after faithfully flat base change and is trivial for the cyclic permutation of the left hand side of $(+)$.

If the first two conditions hold, then the morphism

$$\operatorname{Spec} S \xrightarrow{\operatorname{Id}_{\operatorname{Spec} S} \underset{\operatorname{Spec} R}{\times} \operatorname{Spec} F^n} \operatorname{Spec} S \underset{\operatorname{Spec} R}{\times} \operatorname{Spec} S$$

is, by [GD67, Proposition 17.4.9], an isomorphism to a connected component. Therefore, $(+)$ is a local isomorphism and to see that it is an isomorphism it is sufficient to verify that it is a bijection on geometric points, which follows from the first two conditions. □

Lemma 3. *Let S be an R-algebra generated by a single element $T \in S$ as an R-algebra and which is free of rank d as an R-module, and let F be an automorphism of S which identically acts on R and satisfies $F^d = \operatorname{Id}_S$. Then the pair (S, F) is a FCE extension of degree d of R if and only if for each prime divisor p of d, the element $T - F^{d/p}(T)$ is a unit in S.*

Proof. Since the coequalizer of Id_S and $F^{d/p}$ in the category of rings is $S/\langle T - F^{d/p}(T)\rangle$, the Spec of this quotient is the equalizer of identity and $\operatorname{Spec} F^{d/p}$ in the category of schemes and the condition is a reformulation of the second condition of lemma 2. □

Lemma 4. *Let (S_1, F_1) and (S_2, F_2) be FCE-extensions of degrees $d_1 | d_2$ of an Artinian ring R, and let $S_1 \xrightarrow{\sigma} S_2$ be a morphism of R-algebras satisfying $F_2\sigma = \sigma F_1$. Then σ is injective, and $\sigma(S_1)$ as an R-module is a direct summand of $\sigma(S_2)$.*

Proof. Let $\bar{\mathfrak{k}}$ be the algebraic closure of the residue field of a maximal ideal $\mathfrak{m}$ of R. Since S_2 is a free R-module finite of rank $d_2 > 0$,

$\big(\operatorname{Spec} S_2\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ is not empty. Since F_1 acts on $\big(\operatorname{Spec} S_1\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ transitively and the morphism σ is "Frobenius"-equivariant, this implies the surjectivity of $\big(\operatorname{Spec} S_2\big)(\operatorname{Spec} \bar{\mathfrak{k}}) \xrightarrow{\sigma} \big(\operatorname{Spec} S_1\big)(\operatorname{Spec} \bar{\mathfrak{k}})$. Thus, σ maps the preimage of $\{\mathfrak{m}\}$ in $\operatorname{Spec} S_2$ surjectively to its preimage in $\operatorname{Spec} S_1$. Since this holds for all $\mathfrak{m} \in \operatorname{Spec} R$, $\operatorname{Spec} \sigma$ is surjective, thus dominant, and σ injective. The cokernel of σ has finite projective dimension as an R-module and is thus projective, by the Auslander-Buchsbaum equation [Mat86, Theorem 19.1]. It follows that $\sigma(S_1)$ is a direct summand of the R-module S_2. □

Lemma 5. *Let $(n_k)_{k=1}^K$ be pairwise coprime natural numbers, $n = \prod_{k=1}^K n_k$, (S_k, F_k) FCE-extensions of degree n_k of an Artinian ring R, S an R-algebra which is free of rank n as an R-module and F an endomorphism of S as an R-algebra. Let $S_k \xrightarrow{\phi_k} S$, $1 \le k \le K$, be morphisms of R-algebras such that $\phi_k\big(F_k(s)\big) = F\big(\phi_k(s)\big)$ holds for $1 \le k \le K$ and $s \in S_k$. Then (S, F) is a degree n FCE extension of R, and the morphism*

$$\begin{aligned} \bigotimes_{k=1}^{K} S_k &\to S \\ \bigotimes_{k=1}^{K} s_k &\to \prod_{k=1}^{K} \phi_k(s_k) \end{aligned} \tag{12}$$

is an isomorphism of FCE-extensions of R.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} R$ and $\bar{\mathfrak{k}}$ an algebraic closure of its residue field. Since the action of F on the n_k-element set $\big(\operatorname{Spec} S_k\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ is transitive and the n_k are coprime it follows that F transitively acts on the $\bar{\mathfrak{k}}$-valued points on the left hand side of (12). Since $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$ is not empty and (12) is "Frobenius"-equivariant, it induces a surjection on $\bar{\mathfrak{k}}$-valued points. In view of the remark made before lemma 2, S/R is étale, and (12) induces a bijection on $\bar{\mathfrak{k}}$-valued points as it is surjective and both sets have the same cardinality. It follows that F transitively acts on $\big(\operatorname{Spec} S\big)(\operatorname{Spec} \bar{\mathfrak{k}})$, and (S, F) is an FCE-extension of R. By lemma 4, (12) is injective and since it is a morphism of free modules of the same rank over an Artinian ring is is an isomorphism. □

2.2. **Cyclotomic extensions.** By a primitive s-th root of unity in a ring R, we understand a root ζ of the polynomial

$$\prod_{d|s} (T^d - 1)^{\mu(s/d)},$$

where μ is the Möbius function. Provided that s is a unit in R, it can be shown that ζ is a root of that polynomial if and only if $\zeta^s = 1$ holds in R and $\zeta^d - 1$ is a unit in R, for every natural number $d < s$ dividing s. Let $\mu_s^*(R)$ be the set of primitive s-th roots of 1 in R.

Theorem 2. *Let N and s be coprime positive integers, $L = \mathbb{Q}(\mu_s)$ the s-th cyclotomic field. For $\gcd(k, s) = 1$, let σ_k be the unique automorphism sending each $\zeta \in \mu_s$ to ζ^k, and $L^{\langle N \rangle}$ the subfield of all elements invariant under the automorphism σ_N of $L/\mathbb{Q}$ sending ζ to ζ^N for all $\zeta \in \mu_s$. The following assertions are equivalent:*

- **a:** *If r is a divisor of N, there exists $k \in \mathbb{N}$ such that $r \equiv N^k \bmod s$.*
- **b:** *If r is a prime divisor of N and $\mathfrak{r}$ a prime ideal of $\mathcal{O}_{\mathbb{Q}(\mu_s)}$ containing r, then there is $i \in \mathbb{N}$ such that $\mathrm{Frob}_{\mathfrak{r}/r} \in \mathrm{Gal}\big(\mathbb{Q}(\mu_s) \,/\, \mathbb{Q}\big)$ equals σ_N^i.*
- **c:** *If r is a prime divisor of N and $\mathfrak{r}$ a prime ideal of $\mathcal{O}_{L^{\langle N \rangle}}$ containing r, then the residue field of $\mathfrak{r}$ is isomorphic to $\mathbb{F}_r$.*
- **d:** *There are an FCE extension (S, F) of $\mathbb{Z} \,/\, N\mathbb{Z}$ and a primitive s-th root of unity $\zeta \in S$ such that*

$$F(\zeta) = \zeta^N. \tag{13}$$

- **e:** *The same condition as before, and in addition the degree of S/R equals the multiplicative order of N modulo s and S is generated by ζ as an R-algebra.*

Proof. **a⇒b:** Let $r \equiv N^i \pmod{s}$. We have $\mathrm{Frob}_{\mathfrak{r}/r} = \sigma_r = \sigma_{N^i} = \sigma_N^i$.

b⇒c: Let $\tilde{\mathfrak{r}}$ be a prime ideal of $\mathbb{Q}(\mu_s)$ extending $\mathfrak{r}$. Let $x \in L^{\langle N \rangle}$, then $x \bmod \tilde{\mathfrak{r}} \in \mathbb{F}_r$ since x is invariant under $\mathrm{Frob}_{\tilde{\mathfrak{r}}/r}$, by **b**. Since $\mathfrak{k}(\mathfrak{r})$ is isomorphic to the subfield of $\mathfrak{k}(\tilde{\mathfrak{r}})$ consisting of all $x \bmod \tilde{\mathfrak{r}}$ with $x \in L^{\langle N \rangle}$, **c** follows.

c⇒e: Let $N = \prod_{i=1}^{j} r_i^{k_i}$ be the decomposition of N into prime factors, $\mathfrak{r}_i \in \mathrm{Spec}(\mathcal{O}_{L^{\langle N \rangle}})$ a prime ideal above r_i, and $\mathfrak{N} = \prod_{i=1}^{j} \mathfrak{r}_i^{k_i}$. Then $\mathcal{O}_{L^{\langle N \rangle}}/\mathfrak{N} \cong \mathbb{Z}/N\mathbb{Z}$. Therefore, $S = \mathcal{O}_{\mathbb{Q}(\mu_s)}/\mathfrak{N}\mathcal{O}_{\mathbb{Q}(\mu_s)}$, with the automorphism F defined by the automorphism σ_N of $\mathbb{Q}(\mu_s)/L^{\langle N \rangle}$ and the root of unity ζ given by the image of a generator ζ of μ_s satisfy all conditions.

e⇒d: Trivial.

d⇒a: It is sufficient to prove this for prime divisors r of N. Let $\mathfrak{r} \in \mathrm{Spec}\, S$ be a prime ideal above $r\mathbb{Z}/N\mathbb{Z}$. Let d be the degree of S

over $\mathbb{Z}/N\mathbb{Z}$. The polynomial

$$P(T) = \prod_{k=1}^{d}(T - F^k\zeta) = \prod_{k=1}^{d}(T - \zeta^{N^k})$$

has in fact coefficients in $\mathbb{Z}/N\mathbb{Z}$. Let $\hat{x} = x \bmod \mathfrak{r}$. Then all zeros η of $\hat{P}$ have the form $\hat{\zeta}^{N^l}$, for some integer l. Since $\hat{P}$ has coefficients in $\mathbb{F}_r$, this may be applied to $\eta = \hat{\zeta}^r$. It follows that there exists l with $\hat{\zeta}^r = \hat{\zeta}^{N^l}$, or $r \equiv N^l \pmod{s}$. □

Definition 3. If these equivalent conditions hold, then we say that an s-th cyclotomic extension of $\mathbb{Z}/N\mathbb{Z}$ exists, and any extension with the properties explained in the last point is called an s-th cyclotomic extension.

If S is any FCE-extension of $\mathbb{Z}/N\mathbb{Z}$ and $\zeta \in \mu_s^*(S)$ satisfies (13), then ζ is called a *good s-th root of unity* in S.

Remark 3. This notion of 'cyclotomic extension' is easily seen to be equivalent to Mihailescu's.

Remark 4. Note that if S is any FCE-extension of $\mathbb{Z}/N\mathbb{Z}$ and $\zeta_i \in \mu_{s_i}^*(S)$ are good s_i-th roots of unity and if $\gcd(s_1, s_2) = 1$, then $\zeta_1\zeta_2$ is a good s_1s_2-th root of unity. In particular, an s_1s_2-th cyclotomic extension exists.

2.3. **Relation to Jacobi sums.** Let s be odd and $\zeta \in \mathbb{Q}(\mu_s)$ be a primitive s-th root of unity. If χ is a Dirichlet character modulo s, with values in μ_t, we always put $\chi(n) = 0$ when $\gcd(s, n) \neq 1$. For a Dirichlet character χ modulo s, let

$$\tau(\chi, \zeta) = \sum_{n \in \mathbb{Z}/s\mathbb{Z}} \chi(n)\zeta^n$$

be the Gauß sum. The argument ζ of τ will not be written if it is clear from the context. For another Dirichlet character $\tilde{\chi}$ modulo s such that $\chi\tilde{\chi}$ is a primitive Dirichlet character modulo s, we have

$$\tau(\chi\tilde{\chi}, \zeta)\mathfrak{j}(\chi, \tilde{\chi}) = \tau(\chi, \zeta)\tau(\tilde{\chi}, \zeta) \tag{14}$$

where

$$\mathfrak{j}(\chi, \tilde{\chi}) = \sum_{n \in (\mathbb{Z}/s\mathbb{Z})} \chi(n)\tilde{\chi}(1 - n). \tag{15}$$

More generally, we have

$$\tau(\chi_1, \zeta) \cdot \ldots \cdot \tau(\chi_k, \zeta) = \mathfrak{j}(\chi_1, \ldots, \chi_k)\tau(\chi_1 \cdot \ldots \cdot \chi_k, \zeta) \tag{16}$$

when the τ_i are Dirichlet characters modulo s and $\chi_1 \cdot \ldots \cdot \chi_k$ is primitive, where

$$\mathfrak{j}(\chi_1, \ldots, \chi_k) = \sum_{a_1+\cdots+a_k=1} \chi_1(a_1) \cdot \ldots \cdot \chi_k(a_k) \in \mathbb{Q}(\mu_t) \tag{17}$$

the a_i being $\in \mathbb{Z}/s\mathbb{Z}$.

To convince oneself of (16), let $\chi = \prod_{i=1}^k \chi_i$ and let

$$s_d = \sum_{a_1+\cdots+a_k=d} \chi_1(a_1) \cdot \ldots \cdot \chi_k(a_k)$$

for d in $\mathbb{Z}/s\mathbb{Z}$. We have

$$s_{de} = \chi(e) s_d$$

for $e \in (\mathbb{Z}/s\mathbb{Z})^*$ because of the bijection sending $(a_i)_{i=1}^k$ to $(ea_i)_{i=1}^k$. If $d \notin \mathbb{Z}/s\mathbb{Z}^*$, there exists $e \in (\mathbb{Z}/s\mathbb{Z})^*$ with $\chi(e) \neq 1$ and $ed = d$, and it follows that $s_d = 0$. For $d \in (\mathbb{Z}/s\mathbb{Z})^*$, we obtain $s_d = \chi(d) s_1 = \chi(d)\mathfrak{j}(\chi_1, \ldots, \chi_k)$. But the left hand side of (16) equals

$$\sum_{d \in \mathbb{Z}/s\mathbb{Z}} s_d \zeta^d = \mathfrak{j}(\chi_1, \ldots, \chi_k) \sum_{d \in (\mathbb{Z}/s\mathbb{Z})^*} \chi(d)\zeta^d = \mathfrak{j}(\chi_1, \ldots, \chi_k)\tau(\chi, \zeta).$$

If s is the product of pairwise coprime factors $s_1, \ldots, s_k$ and

$$\chi(n) = \prod_{i=1}^k \chi_i(n), \tag{18}$$

where χ_i is a Dirichlet character modulo s_i, and if $\zeta = \prod_{i=1}^k \zeta_i$, where ζ_i is a primitive s_i-th root of unity, then

$$\tau(\chi, \zeta) = \prod_{i=1}^k \tau(\chi_i, \zeta_i). \tag{19}$$

Note that

$$\tau(\chi_{o,s}, \zeta) = \mu(s), \tag{20}$$

where

$$\chi_{o,s}(n) = \begin{cases} 1 & \gcd(n, s) = 1 \\ 0 & \text{otherwise} \end{cases}$$

and μ is the Möbius function.

Remark 5. Note that (15) is not used when $\chi\tilde{\chi} = 1$. Instead we have, when s is square free and χ primitive,

$$\tau(\chi, \zeta)\tau(\chi^{-1}, \zeta) = s\chi(-1). \tag{21}$$

From this, it follows that $j(\chi,\tilde{\chi})\cdot j(\chi^{-1},\tilde{\chi}^{-1}) = s$ in cases where all occuring Dirichlet characters are primtive and that

$$\mathfrak{j}(\chi_1,\ldots,\chi_k)\mathfrak{j}(\chi_1^{-1},\ldots,\chi_k^{-1}) = s^{k-1}$$

when the χ_k and their product are primtive modulo s. This implies that τ is a unit in every algebra A over the ring of integers in the smallest cyclotomic field containig μ_s and the values of χ such that s is a unit in A. Likewise, if A is an algebra over the ring of integers in the smallest cyclotomic field containing the values of all the χ_i, and if s is a unit in A, and if (16) holds and all the χ_i as well as their product are primitive modulo s, then (17) is a unit in A. This observation will often be used to justify division by Jacobi sums in what follows.

If χ is not primitive but induced from a primitive character modulo the divisor $\tilde{s}$ of s, then (21) becomes

$$\tau(\chi,\zeta)\tau(\chi^{-1},\zeta) = \tilde{s}\chi(-1).$$

By similar considerations as before, (17) is a unit in A if it is defined (i. e., the product of the χ_i is primitive) and if s is a unit in A.

If x is an element of a field of characteristic $r > 0$, we will use $x \in \mathbb{F}_r(\mu_t)$ as a shortcut for the condition that x belongs to the subfield generated by the t-th roots of 1.

Lemma 6. *Let s be square free and N prime to s and χ a Dirichlet character modulo s of order dividing the natural number t. For a Dirichlet character χ modulo s and a prime divisor r of N, the following conditions are equivalent:*

- *For some prime ideal $\mathfrak{r}$ above r of the ring of integers in the field $\mathbb{Q}(\mu_s,\mu_t)$, there exists a $\zeta \in \mu_s^*$ such that the image of $\tau(\chi,\zeta)$ in $\mathfrak{k}(\mathfrak{r})$ is $\in \mathbb{F}_r(\mu_t)$.*
- *For every prime ideal $\mathfrak{r}$ above r of the ring of integers in the field $\mathbb{Q}(\mu_s,\mu_t)$, every $\zeta \in \mu_s^*$ and every $k \in (\mathbb{Z}/t\mathbb{Z})^*$, the image of $\tau(\chi^k,\zeta)$ in $\mathfrak{k}(\mathfrak{r})$ is $\in \mathbb{F}_r(\mu_t)$.*

It will turn out to be useful to have a slightly more general, but a bit more involved lemma:

Lemma 7. *Let s be square free and N prime to s and χ a Dirichlet character modulo s of order dividing the natural number t. For a residue class $e \in \mathbb{Z}/t\mathbb{Z}$ and a prime divisor r of N, the following conditions are equivalent:*

- *For some prime ideal $\mathfrak{r}$ above r of the ring of integers in the field $\mathbb{Q}(\mu_s,\mu_t)$, there exists a $\zeta \in \mu_s^*$ such that the image of $\chi(N)^e\tau(\chi,\zeta)^t$ in $\mathfrak{k}(\mathfrak{r})$ is $\in \mathbb{F}_r(\mu_t)^t$.*

- *For every prime ideal* $\mathfrak{r}$ *above* r *of the ring of integers in the field* $\mathbb{Q}(\mu_s, \mu_t)$*, every* $\zeta \in \mu_s^*$ *and every* $k \in (\mathbb{Z}/t\mathbb{Z})^*$*, the image of* $\chi(N)^{ke}\tau(\chi^k, \zeta)^t$ *in* $\mathfrak{k}(\mathfrak{r})$ *is* $\in \mathbb{F}_r(\mu_t)^t$*.*

Remark 6. It is easy to derive lemma 6 from the special case $e = 0$ of lemma 7. In the special case $e = 0$, the condition on Gauß sums considered in lemma 7 is

$$\tau(\chi, \zeta)^t \bmod \mathfrak{r} \in \mathbb{F}_r(\mu_t)^t,$$

which is clearly implied by the condition $\tau(\chi, \zeta) \bmod \mathfrak{r} \in \mathbb{F}_r(\mu_t)$ studied in lemma 6. To see that the other implication also holds, let $\tau(\chi, \zeta)^t \bmod \mathfrak{r} = x^t$ with $x \in \mathbb{F}_r(\mu_t)$. Then $\tau(\chi, \zeta) \bmod \mathfrak{r} = \xi x$ with some $\xi \in \mu_t$, and we have $\tau(\chi, \zeta) \in \mathbb{F}_r(\mu_t)$.

Proof of lemma 7. It is clear that the second condition implies the first. Also, it follows from (19) and (20) that it is sufficient to consider primitive χ.

Since

$$\tau(\chi, \zeta^l) = \chi(l)^{-1}\tau(\chi, \zeta) \tag{22}$$

for $l \in (\mathbb{Z}/s\mathbb{Z})^*$ and $\chi(l)^t = 1$, the validity of the condition

$A(\chi, \mathfrak{r})$**:** $\quad \tau(\chi, \zeta)^t \bmod \mathfrak{r} \in \mathbb{F}_r(\mu_t)^t$

is really independent of $\zeta \in \mu_s^*$. Since χ is assumed to be primitive and k is coprime to t, it follows that χ^k is also primitive. Thus, $A(\chi, \mathfrak{r})$ implies $A(\chi^k, \mathfrak{r})$ because of (16) and the arguments in remark 5, which justify division by the occuring Jacobi sums.

Finally, if $\tilde{\mathfrak{r}}$ is another prime ideal dividing r, there exists $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\mu_s, \mu_t) \;/\; \mathbb{Q}\big)$ such that $\tilde{\mathfrak{r}} = \sigma\mathfrak{r}$. If the isomorphism of residue fields induced by σ is denoted $\overline{\sigma}$ and $\sigma\big(\chi(n)\big) = \chi(n)^k$, then

$$\overline{\sigma}\big(\tau(\chi, \zeta) \bmod \mathfrak{r}\big) = \tau\big(\chi^k, \sigma(\zeta)\big) \bmod \tilde{\mathfrak{r}},$$

such that $A(\chi, \mathfrak{r})$ implies $A(\chi^k, \tilde{\mathfrak{r}})$. Thus, condition A is also independent of the choice of the prime ideal dividing r. □

Theorem 3. *Let* s *be square free, and let* t *be divisible by* $q - 1$ *for each prime divisor* q *of* s *and such that* N *is coprime to* st *and a* t*-th cyclotomic extension of* $\mathbb{Z}/N\mathbb{Z}$ *exists. Then the following conditions are equivalent:*

- **a:** *An* s*-th cyclotomic extension of* $\mathbb{Z}/N\mathbb{Z}$ *exists.*
- **b:** *For all Dirichlet characters* χ *modulo* s *with* $\chi(N) = 1$ *and all prime divisors* r *of* N*, the equivalent conditions of lemma 6 hold.*

c: *The same condition, but with the additional assumption that the order of χ is a prime power $p^k > 1$.*

Proof. **a⇒b:** We have

$$\tau(\chi,\zeta) = \sum_{\xi\in\mu_t} \xi \sum_{\substack{n\in\mathbb{Z}/s\mathbb{Z}\\ \chi(N)=\xi}} \zeta^n,$$

Since the inner sum is an element of the subfield $L^{\langle N\rangle} \subseteq \mathbb{Q}(\mu_s)$ considered in theorem 2 and the coefficient ξ before the inner sum is $\in \mu_t$, the assertion follows.

b⇒a: Since s is square free, $\mathcal{O}_{\mathbb{Q}(\mu_s)}$ is generated by μ_s^* as an abelian group. Indeed, by [Was97, Theorem 2.6], $\mathcal{O}_{\mathbb{Q}(\mu_s)}$ is generated by μ_s as an abelian group. But for each $d|s$, μ_d^* is contained in the abelian group generated by μ_s^*. This is trivial for $d = s$ and in general follows by downward induction since $\zeta = -\sum_{\eta\in\mu_p^*} \zeta\eta$ when $\zeta \in \mu_d^*$ and p is a prime divisor of s/d, and the summands belong to μ_{dp}^*. It follows that $\phi(s)\mathcal{O}_{L^{\langle N\rangle}}$ is contained in the subgroup of the additive group of $\mathbb{Q}(\mu_s)$ generated by the Gauß periods

$$P_N(\zeta) = \sum_{i=1}^{m} \zeta^{N^i},$$

where m is the multiplicative order of N modulo s and $\zeta \in \mu_s^*$. By theorem 2 and since $\phi(s)$ is invertible modulo N, it suffices to show that $P_N(\zeta) \bmod \mathfrak{r} \in \mathbb{F}_r$, for all prime divisors r of N and all prime ideals $\mathfrak{r}$ of $L^{\langle N\rangle}$ above r. Let $\mathfrak{r}_1$ be a prime ideal of $\mathbb{Q}(\mu_s,\mu_t)$ above $\mathfrak{r}$, and let $\mathfrak{r}_2$ be its intersection with the ring of integers in $\mathbb{Q}(\mu_t)$. Then $\mathbb{F}_r$, $\mathfrak{k}(\mathfrak{r})$ and $\mathfrak{k}(\mathfrak{r}_2)$ are subfields of $\mathfrak{k}(\mathfrak{r}_1)$. By our assumption **b**, we have

$$P_N(\zeta) = \frac{1}{\phi(s)} \sum_{\chi(N)=1} \tau(\chi,\zeta) \in \mathfrak{k}(\mathfrak{r}_2).$$

But $P_N(\zeta)$ is also invariant under the automorphism σ_N of $\mathbb{Q}(\mu_s,\mu_t)$ given by $\sigma_N(\xi) = \xi^N$ for every $\operatorname{lcm}(s,t)$-th root of unity ξ. It follows that $P_N(\zeta) \bmod \mathfrak{r}_2$ is invariant under all automorphisms of $\mathfrak{k}(\mathfrak{r}_2)$ which are induced by σ_{N^i}, where i is such that $\sigma_{N^i}(\mathfrak{r}_2) = \mathfrak{r}_2$. Since a t-th cyclotomic extension of $\mathbb{Z}/N\mathbb{Z}$ exists and because of the second equivalent property in theorem 2, every element of $\mathfrak{k}(\mathfrak{r}_2)$ invariant under such automorphisms is $\in \mathbb{F}_r$, completing the proof of $P_N(\zeta) \in \mathbb{F}_r$ for all $\zeta \in \mu_s^*$.

b⇒c: Trivial.

c⇒b: Let **c** hold, and let χ be any Dirichlet character modulo s. Because of (19) and (20), our assumption that $\tau(\chi,\zeta) \bmod \mathfrak{r} \in \mathbb{F}_r(\mu_t)$

for all χ of prime power order with $\chi(N) = 1$ still holds if s is replaced by a divisor of s. Using this and (19) and (20), we may assume χ to be primitive. By remark 5 it is possible to apply (16) to the decomposition $\chi = \prod_{i=1}^{k} \chi_i$, where χ_i is a Dirichlet character modulo s of order $p_i^{l_i}$ and $p_1 < \cdots < p_k$ are primes. If χ comes from a primitive character $\tilde{\chi}$ modulo a divisor $\tilde{s}$ of s, then the χ_i come from (necessarily primitive) characters $\tilde{\chi}_i$ modulo divisors s_i of s, and it follows from (20), (19) and (16) that

$$(+) \qquad \tau(\chi)\mathfrak{j}(\tilde{\chi}_1, \ldots, \tilde{\chi}_k)\phi\big(\frac{s}{\tilde{s}}\big)^{k-1} = \prod_{j=1}^{k} \tau(\chi_j).$$

By **c**, the factors $\tau(\chi_i)$ are $\in \mathbb{F}_r(\mu_t)$, and by (17) the same holds for $\mathfrak{j}(\tilde{\chi}_1, \ldots, \tilde{\chi}_k)$. The assertion **b** follows. The necessary divison by the second and third factor on the left hand side of (+) is legalized by remark 5 and our assumptions. □

The third condition of the theorem allows us to only work with Dirichlet characters of prime power orders. We would also like to only work with Dirichlet characters modulo the prime factors of s. Then it is necessary to drop the condition $\chi(N) = 1$. The following lemma will be useful:

Let p be a prime not dividing N. We define the saturation exponent $k_{\mathrm{sat}} = k_{\mathrm{sat}}(p, N)$ as follows: If $p > 2$, $p^{k_{\mathrm{sat}}}$ is the largest power of p dividing $N^d - 1$, where d is the multiplicative order of N modulo p. If $p = 2$ and $N \equiv 1 \bmod 4$, $2^{k_{\mathrm{sat}}}$ is the largest power of 2 dividing $N-1$. If $p = 2$ and $N \equiv 3 \bmod 4$, $2^{k_{\mathrm{sat}}}$ is the largest power of 2 dividing $N^2 - 1$.

Let $k \geq k_{\mathrm{sat}}$, and let u_k be the multiplicative order of N modulo p^k. We have $u_k = u_{k_{\mathrm{sat}}} p^{k-k_{\mathrm{sat}}}$ since the multiplicative group of residue classes modulo p^v which are $\equiv 1 \bmod p^u$ is cyclic of order p^{v-u} if $p > 2$ and $v > u > 0$ or $p = 2$ and $v > u > 1$. By our definition of u_k, the exponent of p in the prime factor decomposition of the rational number $\frac{u_k p^k}{N^{u_k}-1}$ is ≥ 0, such that it is possible to form powers $\xi^{\frac{u_k p^k}{N^{u_k}-1}}$, where ξ is a p^l-th root of unity.

Lemma 8. *For a field $\mathfrak{k}$, $k \geq k_{\mathrm{sat}}$, a p^k-th root of unity $\xi \in \mathfrak{k}$, an extension $\mathfrak{l}$ of $\mathfrak{k}$ and $x \in \mathfrak{l}$, we denote by $A(x, k, \xi, \mathfrak{k})$ the condition*

$$x^{p^k} \xi^{\frac{u_k p^k}{N^{u_k}-1}} \in \mathfrak{k}^{p^k}.$$

Then $A(x, k, \xi, \mathfrak{k})$ implies $A(x, l, \xi, \mathfrak{k})$ for $l \geq k$.

Proof. It suffices to prove this for $l = k + 1$. It is possible to simplify $A(x, k, \xi, \mathfrak{k})$ to A_k since the other arguments to A don't change throughout the proof. We have $N^{u_k} = 1 + a_k p^k$, where a_k is not divisible by p. The condition A_k is equivalent to the existence of $y \in \mathfrak{k}$ such that

$$x^{p^k} = y^{p^k} \xi^{-\frac{u_k}{a_k}}. \tag{+}$$

Moreover, we have $u_{k+1} = pu_k$.

If $p > 2$, then $N^{u_{k+1}} \equiv 1 + a_k p^{k+1} \pmod{p^{2k+1}}$, such that $a_{k+1} \equiv a_k \pmod{p^k}$. If $p = 2$, we only have $N^{u_{k+1}} = 1 + a_k p^{k+1} + a_k^2 p^{2k}$ and

$$a_{k+1} \equiv a_k \pmod{p^{k-1}}, \tag{*}$$

but since p divides u_{k+1} and $\xi \in \mu_{p^k}$ the congruence (*) is still sufficient to imply

$$\xi^{-\frac{u_{k+1}}{a_k}} = \xi^{-\frac{u_{k+1}}{a_{k+1}}}.$$

Therefore, the equality

$$x^{p^{k+1}} = y^{p^{k+1}} \xi^{-\frac{pu_k}{a_k}} = y^{p^{k+1}} \xi^{-\frac{u_{k+1}}{a_k}}$$

obtained by raising (+) to the power p yields the analogue of (+) with k replaced by $k + 1$ and implies A_{k+1}. □

If χ is a Dirichlet character modulo a prime q whose order is a prime power $p^l > 1$ and for $k \geq l$, we put $\mathfrak{J}_{p^k}(\chi) = \tau(\chi, \zeta)^{p^k}$. Because of (22), this is independent of ζ. It can be calculated as follows: Since the Dirichlet-characters χ^j, $0 < j < p^l$, are primitive, we have

$$\tau(\chi, \zeta)^j = \tau(\chi^j, \zeta) \prod_{i=1}^{j-1} \mathfrak{j}(\chi, \chi^i) \tag{23}$$

for such j, by induction of j using (14). Together with

$$\tau(\chi, \zeta)\tau(\chi^{-1}, \zeta) = \chi(-1)q,$$

we obtain

$$\mathfrak{J}_{p^l}(\chi) = \chi(-1)q \prod_{j=1}^{p^l-2} \mathfrak{j}(\chi, \chi^j). \tag{24}$$

For $k > l$, we simply use

$$\mathfrak{J}_{p^k}(\chi) = \mathfrak{J}_{p^l}(\chi)^{p^{k-l}}. \tag{25}$$

In particular, $\mathfrak{J}_{p^k}(\chi) \in \mathcal{O}_{\mathbb{Q}(\mu_{p^k})}$.

The Mihailescu certificates for the existence of cyclotomic extensions of $\mathbb{Z}/N\mathbb{Z}$ use these products of Jacobi sums.

Theorem 4. *Let s be square free and t a natural number for which a t-th cyclotomic extension of $\mathbb{Z}/N\mathbb{Z}$ exists, and such that $\gcd(N, st) = 1$.*

In addition, assume that for each prime divisor q of s and for each prime p dividing $q-1$, there exist a Dirichlet character χ modulo q of precise order p^l, where l is the largest exponent such that p^l divides $q-1$, an integer $k \geq \max\bigl(l, k_{\mathrm{sat}}(p, N)\bigr)$ such that p^k divides t, a ring extension S of $\mathbb{Z}/N\mathbb{Z}$ together with a surjective ring homomorphism $\mathcal{O}_{\mathbb{Q}(\mu_{p^k})} \xrightarrow{\Xi} S$, and an element $\sigma \in S$ such that

$$\sigma^{p^k} = \Xi\bigl(\chi(N)^{\frac{up^k}{N^u-1}}\mathfrak{J}_{p^k}(\chi)\bigr), \tag{26}$$

where u is the multiplicative order of N modulo p^k.

Then an s-th cyclotomic extension of $\mathbb{Z}/N\mathbb{Z}$ exists.

Proof. For a prime p dividing $\phi(s)$, let κ_p be the exponent of p in the prime factor decomposition of t, and let u_p be the multiplicative order of N modulo p^{κ_p}. Because of lemma 7 applied with $t = p^{\kappa_p}$, the following two conditions for a Dirichlet character χ of prime power order modulo a divisor $\tilde{s}$ of s are equivalent:

- For all prime divisors r of N, there exist a prime ideal $\mathfrak{r}$ of $K = \mathbb{Q}(\mu_s, \mu_{p^{\kappa_p}})$ dividing r and $\zeta \in \mu_s^*(K)$ such that

$$\tau(\chi, \zeta)^{p^{\kappa_p}}\chi(N)^{\frac{up^{\kappa_p}}{N^{u_p}-1}} \bmod \mathfrak{r} \tag{+}$$

  is a p^{κ_p}-th power in $\mathbb{F}_r(\mu_{p^{\kappa_p}})$.
- For all prime divisors r of N, all prime ideals $\mathfrak{r}$ of K dividing r and all $\zeta \in \mu_s^*(K)$, (+) is a p^{κ_p}-th power in $\mathbb{F}_r(\mu_{p^{\kappa_p}})$.

Since they are equivalent, they define the same predicate $\mathbf{J}(\chi)$.

If $\tilde{s} = s$ and $\chi(N) = 1$, then in view of remark 6, $\mathbf{J}(\chi)$ implies that for every prime ideal $\tilde{\mathfrak{r}}$ of K above a prime divisor r of N and all $\zeta \in \mu_s^*(K)$, the image of $\tau(\chi, \zeta)$ in $\mathfrak{k}(\mathfrak{r})$ is $\in \mathbb{F}_r(\mu_{p^{\kappa_p}})$. Applying this with $\tilde{\mathfrak{r}} = \mathfrak{r} \cap K$, where $\mathfrak{r}$ is any prime ideal of $\mathbb{Q}(\mu_s, \mu_t)$ dividing n, and noting that $\mathbb{F}_r(\mu_{p^{\kappa_p}}) \subseteq \mathbb{F}_r(\mu_t)$, we derive that condition **c** in theorem 3 holds for χ. Therefore, it suffices to show that $\mathbf{J}(\chi)$ holds for all Dirichlet characters χ modulo s of prime power order > 1.

If χ is as in (26), then $\mathbf{J}(\chi)$ holds. In fact, (26) and the surjectivity of Ξ give us that $\tau(\chi, \zeta)^{p^k}\chi(N)^{\frac{up^k}{N^u-1}} \bmod \mathfrak{r}$ is a p^k-th power in $\mathbb{F}_r(\mu_{p^k})$, where $\mathfrak{r}$ is the preimage under Ξ of any prime ideal of S whose preimage in $\mathbb{Z}/N\mathbb{Z}$ is $r\mathbb{Z}/N\mathbb{Z}$. Since $k_{\mathrm{sat}}(p, N) \leq k \leq \kappa_p$, lemma 8 implies the first of the two equivalent characterizations of $\mathbf{J}(\chi)$.

Let χ be the same as before. Then any Dirichlet character modulo q whose order is a prime power $p^m > 1$ has the form χ^j for $0 < j < q$. Because of (23), $\mathbf{J}(\chi^j)$ can be derived from $\mathbf{J}(\chi)$, where remark 5 may

once again be applied to justify the necessary divisions. Because of (20), we also have $\mathbf{J}(\chi_{o,q})$.

We have seen that $\mathbf{J}(\chi)$ holds whenever χ is a Dirichlet character of prime power order modulo a prime divisor of s. If χ is an arbitrary Dirichlet character modulo s whose order is a prime power p^j, then it can be represented as in (18), where the s_i are the prime factors of s and the χ_i are uniquely determined Dirichlet characters modulo s_i whose order is a power of p. Because of (19) and since $\mathbf{J}(\chi_i)$ holds for all i for which the order of χ_i is > 1, we arrive at $\mathbf{J}(\chi)$, proving the theorem. □

In most cases, the saturated cyclotomic extension containing the roots of 1 of order $p^{k_{\mathrm{sat}}}$ modulo N has the same order as the extension containing the p-th root. The only exception is the case $p = 2$ where $N \equiv 3 \pmod 4$. In this case, there is an easy way to check (26) without having to work in an extension of degree 2.

Proposition 2. *Let N and q be both $\equiv 3 \pmod 4$, and let $p^l = 2$. Then, for any S chosen as in the previous theorem, the condition* (26) *is implied by the following condition (which obviously holds when N is a prime satisfying the above assumptions):*

- *One of the two numbers $\pm q$ is a square modulo N.*

Proof. We have

$$\chi(N)^{\frac{up^k}{N^u-1}}\tau(\chi)^{p^k} = q^{2^{k-1}} \tag{+}$$

because of our assumptions. If q is the square of x in $\mathbb{Z}/N\mathbb{Z}$, then (+) is the 2^k-th power of x in S. □

2.4. **Specifying FCE extensions.** In the certficate, FCE extensions (A, F) of $\mathbb{Z}/N\mathbb{Z}$ are given as follows. Data describing the ring extension A are stored in files named *tn*.*c*.`ext`*d*, where *tn* is the twin file name, *c* is 'A' or 'B' depending on whether N is the first or the second component of the twin, and *d* is the decimal representation of the extension degree. The file starts with a string of letters, followed by whitespace, naming the type of ring extension. This is always followed by the decimal representation of the extension degree on the same line.

If the file starts with the string `Kummer`, then the third field on the line is the zero-th coefficient of the Kummer polynomial. For instance, `Kummer 11 3` describes the extension

$$(\mathbb{Z}/N\mathbb{Z})[T] \,/\, (T^{11} + 3).$$

If the file starts with the string `Trionomial`, then the third field is the decimal representation of a positive integer e, the fourth field is the

polynomial coefficient at T^e, and the fifth field the coefficient at T^0. Thus, `Trinomial 11 3 -2 1` describes the extension

$$(\mathbb{Z}/N\mathbb{Z})[T] \,/\, (T^{11} - 2 * T^3 + 1).$$

If the file starts with the string `Generic`, then the initial line contains only that string and the polynomial degree d. This is followed by $d+1$ lines each starting with an initial '`T`', followed without whitespace by the exponent k, followed after a separating space by the coefficient at T^k. These lines are arranged in order of increasing k and include the leading term T^d whose coefficient is 1.

The endomorphism F of the $\mathbb{Z}/N\mathbb{Z}$-algebra A is described in a separate file *tn.c*`.Frob`*d*, where d is the degree of the extension. This contains, on separate lines in order of increasing k, the residue classes f_k modulo N such that F sends T to the image of $\sum_{k=0}^{d-1} f_k T^k$ in A.

It is necessary to check that, for each of the two choices `A` or `B` of c, there is a single FCE extension of $\mathbb{Z}/N\mathbb{Z}$ containing the given extensions as subextensions. To do this, the following tests have to be carried out for each of the FCE extensions given in the certificate.

If an extension (A, F) whose degree $d = p^k$ is a power of a prime p is given, the following tests have to be carried out: Confirm that there is an endomorphism F of A sending T to the polynomial $f = \sum_{k=0}^{d-1} f_k T^k$ specified in the `Frob` file. This is done by verifying that $P(f) = 0$ holds in A. Moreover, confirm that $F^d = \mathrm{Id}_A$ by calculating $F^d(T)$ and confirming that it equals T in A. Finally, confirm (using the Euclidean algorithm) that $F^{d/p}(T) - T$ is invertible in A. This confirms that (A, F) is an FCE-extension of degree d of $\mathbb{Z}/N\mathbb{Z}$, by lemma 3.

To confirm that the extensions whose degrees are powers of p are compatible, determine whether there exist positive $l < k$ such that the extension of degree $e = p^l$ is also specified in the certificate. If this is the case, select the largest number l with this property, and confirm that a file *tn.c*`.sext.`*e.d* is also given, and confirm that it specifies a homomorphism from the degree e to the degree d extension. Let A_e and A_d denote the degree e and d extensions, then the `.sext.`-file should contain the coefficients s_k of an element $s = \sum_{k=0}^{d-1} s_k T^k$ of A_d. Confirm that there is a ring homomorphism σ from A_e to A_d sending T to s. This is done by verifying the equation $P_e(s) = 0$ in A_d, where P_e is the polynomial such that $A_e = \mathbb{Z}/N\mathbb{Z}[T]/P_e$. Moreover, confirm that σ is compatible with the "Frobenius" automorphisms of A_d and A_e. If the image of T under the automorphism F_e of A_e is $f_e = \sum_{k=0}^{e-1} f_{e,k} T^k$ and if f_d plays the same role for F_d and A_d, then compatibility with the Frobenius automorphisms is verified by checking that the equation

$f_e(s) = s(f_d)$ holds in A_d. By lemma 4, σ is injective. This confirms that (A_e, F_e) is isomorphic to a subextension of (A_d, F_d).

If d is not a prime power, decompose it as a product $d = \prod_{i=1}^{j} p_i^{k_i}$ of primes $p_1 < \cdots < p_j$, confirm for each of the prime powers $q = p_i^{k_i}$ that FCE extensions (A_q, F_q) have been given, and that files *tn.c*`.sext.`*q.d* specifying a morphism from (A_q, F_q) to (A_d, F_d) have also been given. As in the prime power case, the `.sext.`-file contains the coefficients s_k of a polynomial $s = \sum_{k=0}^{e-1} s_k T^k$ in order of increasing k. It must be checked that there is a ring homomorphism from A_q to A_d sending $T \in A_q$ to $s \in A_d$ and that this ring homomorphism is compatible with the "Frobenius" actions. This is done in the same way as in the prime power case. After these tests, lemma 5 shows that A_d is indeed an FCE-extension and is, as an FCE-extension, isomorphic to the tensor product of the $F_{p_i^{k_i}}$.

Let $p_1 < \cdots < p_j$ be the list of primes p for which FCE extensions of degree p^d occur in the certificate. Let $p_i^{d_i}$ be the largest power of p_i for which an extension $(A_{p_i^{d_i}}, F_{p_i^{d_i}})$ has been specified. After the tests described in this subsection have been carried out, it is known that

$$\left(\bigotimes_{i=1}^{j} A_{p_i^{d_i}}, \bigotimes_{i=1}^{j} F_{p_i^{d_i}} \right) \tag{27}$$

is an FCE-extension of degree $\prod_{i=1}^{j} p_i^{d_i}$, and that all the FCE extensions provided in the certificate are subextensions of (27).

2.5. **Specifying the cyclotomic certificates.** The number s for which the cyclotomic certificates (i. e., the proofs of validity of condition (26) for the prime factors q of s) modulo the two twin components are given is described in a file *tn*`.s-list` containing one line for each prime factor q of s. The first field is the prime number q, the second field is a primitive root g modulo q, and the remaining fields are the prime factors p of $q - 1$, in increasing order.

To test the validity of this file, test the validity of each line as follows: Confirm (by trial division or table lookup) that the provided factors of $q - 1$ are indeed primes dividing $q - 1$, and that $q - 1$ is a product of powers of these primes. Then, using the prime factorization of $q - 1$ and the given g, confirm that q is indeed prime and g a primitive root modulo q. For reasons which will become apparent later on, we want s to be odd. Therefore, it must also be confirmed that $q \neq 2$. Moreover, it must be confirmed that no prime number q is repeated.

For each prime power $r = p^l$ dividing $q - 1$, and each twin component, check the presence of the certificate `mcert/`*tn.c*`.mcert.`*q.g.*p^l and

confirm its validity as follows. If $p^l = 2$ and $N \equiv 3 \pmod 4$, confirm that the file contains a residue class modulo N whose square is $\pm q$, confirming the condition of proposition 2. Otherwise, determine the multiplicative order u of N modulo p^l, set k equal to the maximum of l and the saturation exponent, read a polynomial $P_u(T)$ specifying a ring extension $S = \mathbb{Z}/N\mathbb{Z}[T] \,/\, P_u(T)$ of degree u from the file *tn.c.*`ext`u, and read a p^k-th root ζ of 1 from *tn.c.*`z`p^k. It is given as the sequence $(z_i)_{i=0}^{u-1}$ of the coefficients z_i of $\zeta = \sum_{i=0}^{u-1} z_i T^i \bmod P_u$, each stored (in order of increasing i) on an indiviual line. Confirm that ζ is indeed a primitive p^k-th root of 1 in S. To verify the surjectivity of Ξ in theorem 4, it must also be confirmed that the powers of ζ generate S as an abelian group. Naturally, these conditions on ζ only have to be confirmed once for each twin component and exponent p^k. Obtain (by direct calculation or by lookup in a collection of p^l-th powers of Gauß sums) the p^l-th power $J = \mathfrak{J}_{p^l}(\chi)$ of the Gauß sum for the Dirichlet character χ modulo q sending g to $e^{\frac{2\pi i}{p^l}}$. Determine the image of J under the ring homomorphism from the ring of integers in $\mathbb{Q}(\mu_{p^l})$ to S sending $e^{\frac{2\pi i}{p^l}}$ to $\zeta^{p^{k-l}}$, calculate the right hand side of (26), and confirm that `mcert/`*tn.c.*`mcert.`$q.g.p^l$ contains the u coefficients of T^k, $0 \le k < u$, of an element of S which is a p^k-th root of that right hand side.

In addition, for each prime divisor p of $\phi(s)$, determine that largest power p^k for which (26) has been confirmed directly or via proposition 2. Determine the appropriate u, read a p^k-th root ζ of 1 from *tn.c.*`z`p^k, and confirm that $F(\zeta) = \zeta^N$ holds for the "Frobenius"-endomorphism F specified in *tn.c.*`Frob`u, where N is the twin component under consideration. Unless this has already been done, it is also necessary to confirm that ζ is a primitive p^k-th root of 1.

After these tests and the tests of the previous subsection, it has been confirmed that for each of the two twin components, the FCE-extension (27) contains, for each of the powers p^k occuring in (26) a good p^k-th root of 1 in the sense of definition 3. Therefore, it also contains a good t-th root of 1, where t is the lcm of those p^k. By theorem 4, an s-th cyclotomic extension exists modulo each twin component.

2.6. **Certification of $\mathfrak{J}_{p^l}(\chi)$.** Since they are the same for each certificate, it is best to provide collection of those elements of the ring of integers of the p^l-th cyclotomic field as a separate file. For the first primality certificates calculated by the authors, they are given in files `Gspk.`$q.g.p^l$, where q is a prime, g is the smallest natural number which is a primitive root modulo q, p a prime divisor of $q-1$ and p^l its largest

power dividing $q-1$. The file contains, on separate lines and in order of increasing k, the rational integers which are the coefficients of a representation of $\mathfrak{J}_{p^l}$ as a linear combination of $\exp\frac{2\pi ik}{p^l}$, $0 \le k < p^l - p^{l-1}$ in order of increasing k. This is done for the Dirichlet character χ modulo q sending g to $\exp\frac{2\pi i}{p^l}$. The correctness of the value can be confirmed by the following theorem, which is inspired by [Mih06a, Lemma 3 in Section 5.1].

Theorem 5. *Let q be a prime number and χ a primitive Dirichlet character modulo q whose order is a power of a prime p. Let p^l be the largest power of p dividing $q-1$. Then $J = \mathfrak{J}_{p^l}(\chi)$ is an element of the ring of integers R in the p^l-th cyclotomic field satisfying the following conditions, which characterize it uniquely:*

- $J \cdot \overline{J} = q^{p^l}$.
- *Let $\mathfrak{p}$ be a prime ideal of R containing q, and let k be the smallest natural number such that*

  $$\chi(x) \equiv x^{-k} \pmod{\mathfrak{p}}$$

  holds for each integer x prime to q. Then the exponent of $\mathfrak{p}$ in the prime ideal decomposition of J is given by $\frac{kp^l}{q-1}$.
- *We have*

  $$J \equiv (-1)^p \pmod{p(\zeta-1)},$$

  where $\zeta \in R$ is a primitive p^l-th root of 1.

Note that the last condition does not depend on ζ.

Proof. The first condition of J follows from the well-known and easy equation $\tau(\chi,\zeta)\cdot\tau(\chi^{-1},\zeta^{-1}) = q$. The second condition is Stickelberger's theorem ([Was97, Proposition 6.13] or [Lan90, Theorem 2.1]). For the third condition, we calculate

$$\begin{aligned}\tau(\chi,\xi)^{p^l} &= \Big(\sum_{k=1}^{q-1}\chi(k)\xi^k\Big)^{p^l}\\ &= \Big(-1+\sum_{k=1}^{q-1}\big(\chi(k)-1\big)\xi^k\Big)^{p^l}\\ &= (-1)^p + \sum_{j=1}^{p^l}\binom{p^l}{j}(-1)^{p-j}\Big(\sum_{k=1}^{q-1}\big(\chi(k)-1\big)\xi^k\Big)^j.\end{aligned}$$

If $j < p^l$, the j-th summand is divisible by $p(\zeta-1)^j$ which in turn is divisible by $p(\zeta-1)$. If $j = p^l$, it is divisible by $(\zeta-1)^{p^l}$ which is also

divisible by $p(\zeta-1)$, because of the well-known relation

$$(+) \qquad \langle \zeta-1\rangle^{p^{l-1}(p-1)} = \langle p\rangle.$$

for the ideal generated by $\zeta-1$.

For uniqueness, note that the first condition implies that all prime divisors of J must contain q. Together with the second condition, this determines the prime ideal decomposition of J, and thus determines J up to a unit. By the first condition, it is also determined up a root of 1. It is known that the group of roots of 1 in R is $\{\pm 1\}\mu_{p^l}$. For instance, this follows from the determination of the degree of $\mathbb{Q}(\mu_n)$ [Was97, Theorem 2.5] since $\phi(ap^l) > \phi(p^l)$ when $a > 1$ unless $a = 2$ and p is odd.

The conditions thus characterize J up to multiplication by an element of $\pm\mu_{p^l}$. If p is odd, then the third condition excludes the minus sign. Therefore, the conditions characterize J up to multiplication by some $\xi \in \mu_{p^l}$. If ξ is not 1, it is a primitive p^j-th root of 1, for some j which is positive but $\leq l$. Then $(\xi-1)R = (pR)^{\frac{1}{(p-1)p^{j-1}}}$ by $(+)$, where the fractional power may be taken in the ideal group of R and the exponent is always ≤ 1. But $p(\zeta-1)R = (pR)^{1+\frac{1}{(p-1)p^{l-1}}}$ and the exponent is always > 1. Thus, the third condition fails if J is replaced by ξJ, finishing the proof of uniqueness. □

Note that if the first property of the theorem holds, then the validity of the second property for a prime ideal $\mathfrak{p}$ is equivalent to its validity for $\overline{\mathfrak{p}}$. This means that the second property only has to be verified for half of the prime ideals. Another possibility is to only verify the same one-sided inequality for the prime ideal exponent of both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$.

3. Mihailescu exponent congruences

Let $(K, E_1, E_2, \mu_1, \mu_2)$ be a Mihailescu twin, where E_k is defined modulo N_k. Let r_k be as in theorem 1. If both rings $\mathbb{Z}/N_k\mathbb{Z}$, $k \in \{1;2\}$, have s-th cyclotomic extensions, then there exist exponents $\lambda_k \in \mathbb{N}$, $k \in \{1;2\}$, such that

$$(28) \qquad r_k \equiv N_k^{\lambda_k} \pmod{s}.$$

Let o_k be the multiplicative order of N_k modulo s. The last crucial ingredient of the test is a method of narrowing down the choices for λ_k and ensuring that at least one r_k must be larger than the bound from theorem 1, bypassing the trial division step or the Lenstra step of the classical Jacobi sum primality test. It is based upon an elliptic version of definition 3. Since we will not use analogues of theorem 3 or theorem 4, we only introduce the analog of (13).

3.1. **Good division points.** Let $\mathcal{E}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ over $\mathbb{Z}/N\mathbb{Z}$, let $I \subseteq \mathcal{O}_K$ be an ideal, and let S be an $\mathbb{Z}/N\mathbb{Z}$-algebra. An I-divsion point is a point $P \in \mathcal{E}(S)$ such that $\iota \cdot P = 0$ for all $\iota \in I$. The set of I-division points will be denoted $\mathcal{E}(S)_I$. We call P primitive if in addition the morphism

$$(\mathcal{O}_K/I) \times \operatorname{Spec}(S) \to \mathcal{E} \bigtimes_{\operatorname{Spec}(\mathbb{Z}/N\mathbb{Z})} \operatorname{Spec} S \tag{29}$$

whose restriction to $(\iota \bmod I) \times \operatorname{Spec}(S)$ equals ιP is a closed immersion. In (29), the left hand side is viewed as a disjoint union, taken over the set $\mathcal{O}_K/I$, of copies of $\operatorname{Spec}(S)$.

Recall the notion of a free, cyclic étale extension of $\mathbb{Z}/N\mathbb{Z}$ from definition 2.

Let $(K, E_1, E_2, \mu_1, \mu_2)$ be a Mihailescu twin. Let $N_k = N_{K/\mathbb{Q}}(\mu_k)$ be the number modulo which the elliptic curve $\mathcal{E}_k$ with complex multiplication is defined.

Definition 4. Let I be prime to $\mu_1\mu_2$. A primitive I-division point P of $\mathcal{E}_k$ with values in the FCE-extension (S, F) of $\mathbb{Z}/N_k\mathbb{Z}$ is called good if it is primitive and its image $F(P)$ under the automorphism F of S equals $\mu_k P$. In the case where $I = \ell\mathcal{O}_K$, where ℓ is a natural number, we speak of a good ℓ-division point.

The application of this notion to narrow down the choices for the exponents in (28) is based upon the following proposition, which should be compared with theorem 2.

Proposition 3. *Let $(K, E_1, E_2, \mu_1, \mu_2)$ be a Mihailescu twin and $k \in \{1; 2\}$ such that $\mathcal{E}_k$ has good a I-division point P with values in an FCE-extension (S_k, F_k) of $\mathbb{Z}/N_k\mathbb{Z}$. If r is a prime divisor of N_k and $\pi_r \in \mathcal{O}_K$ the corresponding Frobenius element as in the formulation of theorem 1, then there exists a natural number l with $\pi_r \equiv \mu_k^l \pmod I$.*

Proof. We use the language of effective relative Cartier divisors as in [KM85]. Let $\mathcal{E}_{k,A} = \mathcal{E}_k \bigtimes_{\operatorname{Spec}\mathbb{Z}/N_k\mathbb{Z}} \operatorname{Spec} A$ denote the base-change of $\mathcal{E}_k$ to $\mathbb{Z}/N\mathbb{Z}$-algebras A. Let $D \subset \mathcal{E}_{k,S_k}$ be an effective relative Cartier divisor which is invariant under the automorphism of $\mathcal{E}_{k,S_k}$ defined by F_k. Let the degree of S_k be d. Since there is an isomorphism between $\operatorname{Spec} S_k \times \operatorname{Spec} S_k$ and the disjoint union of d copies of $\operatorname{Spec} S_k$ which equals $\big(\mathrm{Id}, \operatorname{Spec}(F_k^j)\big)$ on the j-th copy, the "Frobenius"-invariance of D implies that there is a unique structure of a descent datum for $\mathcal{E}_{k,S_k}/\mathcal{E}_k$ on the sheaf of ideals $\mathcal{I}_D$ defining D such that $\mathcal{I}_D \to \mathcal{O}_{\mathcal{E}_{k,S_k}}$ is a morphism of descent data. By faithfully flat descent, D descends to $\mathcal{E}_k$ in

the sense that there is a unique effective relative Cartier divisor $\tilde{D} \subset \mathcal{E}_k$ whose preimage in $\mathcal{E}_{k,S_k}$ equals D.

Let D be as before and let r be the divisor of N_k which is under consideration, then there exists a maximal ideal of S_k whose residue field $\mathfrak{k}$ has characteristic r. The closed embedding $\operatorname{Spec}\mathfrak{k} \to \operatorname{Spec} S_k$ defines a closed embedding $\mathcal{E}_{k,\mathfrak{k}} \to \mathcal{E}_{k,S_k}$ which allows us to restrict divisors on $\mathcal{E}_{k,S_k}$ to $\mathcal{E}_{k,\mathfrak{k}}$. The fact that D is the preimage of a $\tilde{D}$ which is defined over $\mathbb{Z}/N_k\mathbb{Z}$ implies that $[\pi_r]_{\mathcal{E}_{k,\mathfrak{k}}}$ maps the preimage $D_\mathfrak{k}$ of D in $\mathcal{E}_{k,\mathfrak{k}}$ to itself. In tedious detail this can be seen as follows. The absolute Frobenius $\mathfrak{F}_{\mathcal{E}_{k,\mathfrak{k}}}$ as an endomorphism of $\mathcal{E}_{k,\mathfrak{k}} \cong \mathcal{E}_{k,\operatorname{Spec}\mathbb{F}_r} \times \operatorname{Spec}\mathfrak{k}$ is given by $\mathfrak{F}_{\mathcal{E}_{k,\operatorname{Spec}\mathbb{F}_r}} \times \mathfrak{F}_{\operatorname{Spec}\mathfrak{k}}$, and because of its definition maps any closed subscheme to itself. Since $\mathfrak{F}_{\mathcal{E}_k} = [\pi_r]$ it follows that

$$[\pi_r]_{\mathcal{E}_{k,\operatorname{Spec}\mathbb{F}_r}} \times \mathfrak{F}_{\operatorname{Spec}\mathfrak{k}} = [\pi_r]_{\mathcal{E}_{k,\operatorname{Spec}\mathfrak{k}}} \circ \left(\operatorname{Id}_{\mathcal{E}_k} \times \mathfrak{F}_{\operatorname{Spec}\mathfrak{k}}\right)$$

maps $D_\mathfrak{k}$ to itself. But the fact that D may be defined over $\mathbb{Z}/N_k\mathbb{Z}$ implies that $\operatorname{Id}_{\mathcal{E}_k} \times \mathfrak{F}_{\operatorname{Spec}\mathfrak{k}}$, which is an automorphism of $\mathcal{E}_{k,\mathfrak{k}}$, maps $D_\mathfrak{k}$ isomorphically to itself. Thus, $[\pi_r]_{\mathcal{E}_{k,\operatorname{Spec}\mathfrak{k}}}$ maps $D_\mathfrak{k}$ to itself.

Let o be the multiplicative order of μ_k modulo I. We apply the previous considerations to the divisor $D = \sum_{l=1}^{o} [\mu^l]_{\mathcal{E}_k,S_k} P$ on $\mathcal{E}_{k,S_k}$, which is F_k-invariant. Since $P\,|_{\operatorname{Spec}\mathfrak{k}}$ factors over $D_\mathfrak{k} = \sum_{l=1}^{o} [\mu^l]_{\mathcal{E}_{k,\mathfrak{k}}} P\,|_{\operatorname{Spec}\mathfrak{k}}$, $[\pi_r]_{\mathcal{E}_{k,\mathfrak{k}}} P\,|_{\operatorname{Spec}\mathfrak{k}}$ also factors over $D_\mathfrak{k}$. Since $\operatorname{Spec}\mathfrak{k}$ is integral, it follows that there exists $l \in [1,o] \cap \mathbb{Z}$ with $[\pi_r]_{\mathcal{E}_{k,\mathfrak{k}}} P\,|_{\operatorname{Spec}\mathfrak{k}} = [\mu^l]_{\mathcal{E}_{k,\mathfrak{k}}} P\,|_{\operatorname{Spec}\mathfrak{k}}$. Since (29) is a closed immersion, this implies $\pi_r \equiv \mu^l \pmod{I}$ as stated. □

Corollary 1. *Let $(K, E_1, E_2, \mu_1, \mu_2)$ be a Mihailescu twin. Let s be odd and square free, and assume that both rings $\mathbb{Z}/N_k\mathbb{Z}$ have an s-th cyclotomic extension. Let o_k be the multiplicative order of N_k modulo s. Let (S_k, F_k) be an FCE-extension of $\mathbb{Z}/N_k\mathbb{Z}$, and let $\tilde{s}$ be a divisor of s such that both curves $\mathcal{E}_k$ have a good $\tilde{s}$-division point with values in S_k, and let $\tilde{o}_k$ be the multiplicative order of N_k modulo $\tilde{s}$.*

Under these assumptions, if r_1 and r_2 are as in theorem 1 and $\lambda_{1,2}$ as in (28)*, there is a solution to the congruence*

$$\mu_1^{l_1} + \mu_2^{l_2} \equiv 1 \pmod{\tilde{s}\mathcal{O}_k} \tag{30}$$

such that $\lambda_k \equiv l_k \pmod{\tilde{o}_k}$.

Proof. Let $\rho_k = \pi_{r_k}$. We have

$$\rho_1 + \rho_2 = 1 \tag{31}$$

as part of the conditions which the Mihailescu twin (5) must satisfy. Because of proposition 3, there exists $l_k \in \mathbb{N}$ such that

$$\rho_k \equiv \mu_k^{l_k} \pmod{\tilde{s}\mathcal{O}_K}. \tag{32}$$

This implies

$$r_k \equiv N_k^{l_k} \pmod{\tilde{s}}$$

by taking norms. Since (28) implies $r_k \equiv N_k^{\lambda_k} \pmod{\tilde{s}}$, we have $\lambda_k \equiv l_k \pmod{\tilde{o}_k}$. By (31) and (32), the pair (l_1, l_2) is a solution to (30). □

Corollary 2. *We retain the notations and assumptions of the previous corollary and assume that theorem 1 is applicable. Let* $B = \left\lfloor 2(\sqrt[4]{\min(N_1, N_2)} + p - 2) \right\rfloor$*, where* p *is as in the aforementioned theorem. We also assume that for every pair* (λ_1, λ_2) *of residue classes* $\lambda_k \bmod o_k$ *for which there exists a solution* (l_1, l_2) *to* (30) *such that* $\lambda_k \equiv l_k \pmod{\tilde{o}_k}$*, the smallest non-negative representative* r *of the residue class of* $N_1^{\lambda_1} - N_2^{\lambda_2}$ *modulo* s *is* $\geq B$ *if it is even and* $\leq s - B$ *if it is odd.*

Then N_1 *and* N_2 *are prime.*

Proof. Indeed, if r_1 and r_2 are as in theorem 1 and $\lambda_{1,2}$ as in (28), then by the previous corollary our assumption must be applicable to the smallest non-negative representative r of the residue class of $N_1^{\lambda_1} - N_2^{\lambda_2}$ modulo s. If r is odd, it is positive and since s is odd we may exchange N_1 and N_2 and replace r by $s - r$. Therefore, let r be even.

We have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\rho_1) = r_1 + 1 - r_2 \equiv N_1^{\lambda_1} + 1 - N_2^{\lambda_2} \equiv r + 1 \pmod{s} \tag{33}$$

Since the left hand side of (33) is an odd number and $r + 1$ has the smallest absolute value of any odd representative of its residue class modulo s, we have

$$|\Re\rho_1| = \frac{1}{2}\left|\mathrm{Tr}_{K/\mathbb{Q}}(\rho_1)\right| \geq \frac{B+1}{2} > \sqrt[4]{\min(N_1, N_2)} + p - 2,$$

contradicting the bound $\sqrt{b} + p - 2 \leq \sqrt[4]{\min(N_1, N_2)} + p - 2$ for $|\rho_1| = \sqrt{r_1}$ from theorem 1. □

Remark 7. The use of Hasse's inequality for points on elliptic curves over finite fields is similar to the proposal in [Mih06b, (19)]. It seems likely that a quicker way is to use the fact that the Mihailescu congruence (30) tends to have but a few solutions, together with a method for finding all divisors in a given residue class such as [CHGN08] (improving [Len84]). For this, cyclotomic certificates should be produced for s_1 modulo N_1 and s_2 modulo N_2 where $s_1 > N_1^{1/4+\epsilon}$ and $s_2 = \tilde{s}$ is the product of the prime numbers q for which good elliptic torsion points are specified. It is then necessary to rule out the existence of non-trivial divisors of N_1 in the residue classes of $N_1^{\lambda_1}$ modulo s_1 for which (30) has a solution (l_1, l_2) with $l_1 \equiv \lambda_1 \pmod{\tilde{o}_1}$. Of course, the

roles of N_1 and N_2 may be exchanged, such that most of the Jacobi sum certificates only have to be calculated for the twin component for which this is easiest to do, and for which they take fewer disk space.

We will finish the subsection with a few remarks about how to effectively specify data which prove the existence of good elliptic torsion points. Firstly, it is sufficient to treat the prime factors of $\tilde{s}$ separately:

Remark 8. If I_ι, for $\iota \in \{1; 2\}$, are coprime ideals of $\mathcal{O}_K$ and $P_\iota \in \mathcal{E}(S_k)$ good I_ι-division points, then $P_1 + P_2 \in \mathcal{E}(S_k)$ is a good $I_1 I_2$-division point.

In practice, S_k is given as the tensor product of many factors with small prime power orders, but for each individual prime factor of $\tilde{s}$ only some of these factors are needed.

The necessary work may be further reduced by an application of the Weil pairing. Before we describe it, note that prime numbers which split in $\mathcal{O}_k$ are far more desirable as factors of $\tilde{s}$ than those which stay prime. This is so because the congruences (30) are far more likely to have many solutions if $\mathcal{O}_K/\tilde{s}\mathcal{O}_K$ has a large cyclic factor. Let, therefore, q be a prime number which splits as $q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}}$ with $\mathfrak{q} \neq \overline{\mathfrak{q}}$. The following is an easy application of the Weil pairing ([KM85, 2.8.5]):

Lemma 9.
- *If $P \in \mathcal{E}_k(S_k)_\mathfrak{q}$ is a primitive $\mathfrak{q}$-division point, then the Weil pairing W induces an isomorphism*
$$\begin{aligned} \mathcal{E}(S_k)_{\overline{\mathfrak{q}}} &\to \mu_q(S_k) \\ Q &\to W(P, Q). \end{aligned}$$
- *If $\mathcal{E}_k$ has a good $\mathfrak{q}$-division point defined over S_k and if S_k contains a good q-th root of unity, then $\mathcal{E}_k$ also has a good $\overline{\mathfrak{q}}$-division point defined over S_k and therefore (Remark 8) a good q-division point defined over S_k.*

3.2. **Specifying good division points.** The number $\tilde{s}$ is specified in a file *tn*`.ell-q` listing its prime factors, one factor on each line. To confirm its validity, confirm that each of the listed numbers q is a prime divisor of *tn*`.s-list`. For the way of specifying good division points described below, it is also necessary to verify that q splits into two distinct prime ideals $\mathfrak{q}_0$ and $\mathfrak{q}_1$ of the ring of integers in $\mathbb{Q}(\sqrt{-D})$, where D is the number obtained from the twin file *tn*. We label the two prime ideals in such a way that $\mathfrak{q}_i$ contains $\sqrt{-D} - r$ where $r \geq 0$ and $r < q$ and $r \equiv i \bmod 2$.

Moreover, confirm that no prime number occurs twice in *tn*`.ell-q`, and let $\tilde{s}$ be the product of the primes in *tn*`.ell-q` and s the product

of the primes q which are the first fields of the lines of *tn*.`s-list`. Let o_k and $\tilde{o}_k$ be as in corollary 1. For each pair (λ_1, λ_2) of residue classes λ_k modulo o_k for which there exists a solution (l_1, l_2) to (30) such that $\lambda_k \equiv l_k \pmod{\tilde{o}_k}$, confirm that the smallest non-negative representative r of the residue class of $N_1^{\lambda_1} - N_2^{\lambda_2}$ modulo s satisfies the condition of corollary 2.

Let c be 'A' or 'B' and let N be the correspoding twin component. Let x and y be the integers specified in *tn* with lines starting with 'X' and 'Y', and let ν be $\frac{x+y\sqrt{-D}}{2}$ if c is 'A' and $\frac{2-x-y\sqrt{-D}}{2}$ if c is 'B'. Thus, ν is an element of $\mathbb{Q}(\sqrt{-D})$ with norm N. Moreover, let

$$\mathcal{E}: \quad y^2 = x^3 + ax + b$$

be the elliptic curve with coefficients a and b in $\mathbb{Z}/N\mathbb{Z}$ specified in *tn.c*.`curve0`, with the complex multiplication specified in *tn.c*.`CMdat`. To confirm that it has a good $\tilde{s}$-division point with values in (27), it is by remark 8 sufficient to show that for each prime divisor q of $\tilde{s}$ there is a good q-division point. Also by remark 8, this may be done by specifying good $\mathfrak{q}_i$-division points for $i = 0$ and $i = 1$. By the Weil pairing argument of lemma 9, it is also sufficient to specify a good division point for one of the $\mathfrak{q}_i$ in addition to a good q-th root of 1.

A good q-th root of 1 is specified in a file *tn.c*.`cext`q together with files *tn.c*.`csext`$q.p^k$ for each maximal prime power divisor p^k of the multiplicative order o of N modulo q. To check the validity, read a polynomial $P[T]$ (whose order must be o) from *tn*.`cext`q. Confirm that the image of T in $S = \mathbb{Z}/N\mathbb{Z}[T]/P(T)$ is a primitive q-th root of 1 and that T^N also is a zero of the polynomial P. It is then clear that there is an endomorphism F of S sending T to T^N. For each maximal prime divisor p^k of o, confirm the presence of files *tn*.`ext`p^k and *tn*.`Frob`p^k. As was confirmed by the tests in subsection 2.4, these specify an FCE extension $(S_{p^k} = \mathbb{Z}/N\mathbb{Z}[T]/P_{p^k}(T), F_{p^k})$ which is a subextension of (27). Moreover, confirm that a file *tn.c*.`csext`$q.p^k$ exists and that it contains, in order of increasing j, the coefficients s_j of a polynomial $s(T) = \sum_{j=0}^{o-1} s_j T^j$ with coefficients in $\mathbb{Z}/N\mathbb{Z}$. This must be subjected to the same tests described for a *tn.c*.`sext`-file in subsection 2.4. More precisely: Confirm that the image of s in S is a zero of the polynomial P_{p^k}. This implies the existence of a ring homomorphism $S_{p^k} \xrightarrow{\sigma} S$ sending T to s. Moreover, confirm the equality $f^{(p^k)}(s) = s(T^N)$ in S, where $f^{(p^k)} \in \mathbb{Z}/N\mathbb{Z}[T]$ is the polynomial of degree $< p^k$ whose image in S_{p^k} equals the image of T under F_{p^k}. This implies that σ is compatible with the "Frobenius"-maps. After this has been verified for all maximal prime power divisors p^k of o, it is clear that $(S, F) \cong \bigotimes_p (S_{p^k}, F_{p^k})$ as

FCE-extensions of $\mathbb{Z}/N\mathbb{Z}$, and that (27) contains a good q-th root of 1.

A good $\mathfrak{q}_i$-torsion point is always specified in a file *tn.c*.`etdat`i.q which starts with the letter 'O' followed by some whitespace followed by the decimal representation of a positive integer o followed by the newline character. While o will normally be equal to the multiplicative order of ν modulo $\mathfrak{q}_i$, it is not necessary to check this. Let d be o if o is odd and $o/2$ if o is even. The initial line of *tn.c*.`etdat`i.q is always followed by $d+1$ lines. In order of increasing k and beginning with $k = 0$, these lines start with the letter 'g' followed without whitespace by the decimal representation of k. After some whitespace, this is followed by a residue class g_k modulo N with which the line terminates. Let $g = \sum_{k=0}^{d} g_k X^k$. The coefficient g_d must always be 1. If o is even, the file *tn.c*.`etdat`i.q terminates after these lines. Otherwise, it contains d lines starting with the letter 'Y' directly followed by the decimal representation of k directly followed by a residue class y_k modulo N with which the line terminates, where k runs from 0 to $d-1$. The file terminates at this point. Let $y = \sum_{k=0}^{d-1} y_k X^k$.

Let $\tilde{S} = \mathbb{Z}/N\mathbb{Z}[X] \,/\, g(X)$. If o is odd, let $S = \tilde{S}$, and let $P = (X, y)$. If o is even, let

$$S = \tilde{S}[Y] \,/\, \big(Y^2 - X^3 - aX - b\big),$$

and let $P = (X, Y)$. In the former case, confirm that P is on the curve $\mathcal{E}$. In the case where o is even, this is always the case in view of our definitions. In both cases, we thus have an S-valued point $P \in \mathcal{E}(S)$. Confirm that it is a q-torsion point. It is also necessary to confirm that it is $\mathfrak{q}_i$-torsion. To do this, let a be the integer specified in *tn.c*.`CMdat`. The `CMdat`-file thus specifies the action of $\alpha = \frac{a+\sqrt{-D}}{2}$ on the curve $\mathcal{E}$ as an isogeny chain (8). To confirm that P is $\mathfrak{q}_i$-torsion, apply the chain links in the chain (8) to P and check that the final result equals $\rho \cdot P$, where $\rho \in \mathbb{Z}$ is some representative of the residue class of α modulo $\mathfrak{q}_i$, preferrably the one of smallest absolute value. It has then been confirmed that P is a $\mathfrak{q}_i$-torsion point.

It is also necessary to calculate $r \cdot P$, where $r \in \mathbb{Z}$ is some representative of the residue class of ν modulo $\mathfrak{q}_i$. If o is odd, then the result has the form $(\phi(X), \chi(X))$, where ϕ and χ are polynomials of degree $< d$ in X with coefficients in $\mathbb{Z}/N\mathbb{Z}$. If o is even, then the result has the form $\big(\phi(X), \chi(X)Y\big)$ where ϕ and χ are as in the former case. In both cases, it is necessary to confirm that there is an endomorphism F of the ring $\tilde{S}$ sending X to $\phi(X)$. This is done by confirming that $\phi \bmod g$ is a zero of the polynomial g. In the case where o is even, it

is also necessary to confirm that F extends to an endomorphism of S which for the sake of simplicity will also be called F. This is done by confirming that $\chi^2 = \phi^3 + a\phi + b$ holds in $\tilde{S}$. In the case where o is odd, it is instead necessary to confirm that $F(y) = \chi$ holds in $S = \tilde{S}$. This is done by calculating $y\big(\phi \bmod g\big)$ and confirming that it equals $\chi \bmod g$. In both cases, we have confirmed that we have an endomorphism F of S and that $F(P) = \nu \cdot P$.

Note that in both cases S is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank o. It is finally necessary to give, for each prime divisor p of o and its maximal power p^k dividing o, a morphism $(S_{p^k}, F_{p^k}) \xrightarrow{\mathfrak{s}} (S, F)$, where (S_{p^k}, F_{p^k}) is the pair specified in *tn.c.*`extp`^{k} and *tn.c.*`Frobp`^{k}, S_{p^k} being $\mathbb{Z}/N\mathbb{Z}[T] \;/\; P_{p^k}(T)$ and F_{p^k} sending T to $\phi_{p^k}(T) \bmod P_{p^k}$. The morphism $\mathfrak{s}$ is specified in a file *tn.c.*`esext`$i.q.p^k$ which always contains, with j running from 0 to $d-1$, d lines starting with the letter 'X', directly followed by the decimal representation of j, followed after some whitespace by a residue class σ_j modulo N terminating the line. If $p > 2$, the file stops at this point. Otherwise, it also contains $d-1$ lines which, with j running from 0 to $d-1$, start with the string `"YX"`, directly followed by the decimal representation of j, followed after some whitespace by a residue class τ_j modulo N terminating the line. The file terminates at this point. We always put $\sigma = \sum_{j=0}^{d-1} \sigma_j X^j$. If $p = 2$, we also put $\tau = \sum_{j=0}^{d-1} \tau_j X^j$. The morphism $\mathfrak{s}$ is uniquely determined by the property that it sends T to $\sigma(X)$ if $p > 2$ and to $\sigma(X) + \tau(X)Y$ if $p = 2$. It must be confirmed that such a morphism exists and is "Frobenius"-compatible. For existence, confirm that $\sigma \bmod g$ is a zero of the polynomial P_{p^k} if $p > 2$. If $p = 2$, it is instead necessary to calculate the value of P_{p^k} at $\sigma(X) + \tau(X)Y$ modulo $Y^2 - X^3 - aX - b$ and modulo $g(X)$ and to confirm that it is 0. In both cases, it has then been confirmed that there is a unique ring homomorphism $\mathfrak{s}$ from S_{p^k} to S with the aforementioned image of $T \in S_{p^k}$.

To confirm "Frobenius"-compatibility when $p > 2$, confirm that the identity $\sigma(\phi) = \phi_{p^k}(\sigma)$ holds in $\tilde{S}$. If $p = 2$, confirm the identity

$$\sigma(\phi) + \tau(\phi) \cdot \chi = \phi_{p^k}\big(\sigma(X) + \tau(X)Y\big)$$

in S. After the files *tn.c.*`esext`$i.q.p^k$ have passed these tests, we know in view of lemma 5 that (S, F) is isomorphic to $\bigotimes_p \big(S_{p^k}, F_{p^k}\big)$, and thus to a subalgebra of (27) as an FCE-algebra.

For each q listed in *tn*.`ell-q`, and for both possible values 'A' and 'B' of c, it is necessary that for at least one $i \in \{0; 1\}$, the file *tn.c.*`etdat`$i.q$ and all necessary *tn.c.*`esext`$i.q.p^k$ are present and pass the above tests. Moreover it is necessary that either these files are present and correct

for the other value of i as well, or that $tn.c.\texttt{cext}.q$ with the necessary files $tn.c.\texttt{csext}.q.p^k$ is also present and passes the tests described before we started the description of the elliptic torsion data.

After all the tests from subsection 1.3, subsection 1.4, subsection 2.4, subsection 2.5 (with values of $\mathfrak{J}_{p^k}(\chi)$ whose correctness has been established by calculating them or by applying theorem 5 to a collection of p^k-th powers of Gauß sums provided with the certificate) have been finished together with the tests of this subsection, the primality of the input number follows by a combination of corollary 2, theorem 4 and the fact that the Goldwasser-Kilian chain supplied in $tn.\texttt{ecpp}$ reduces the primality of its intial term to the primality of the term for which a Mihailescu twin has been specified. In a solemn language worthy of all the hard mathematics and all the CPU-months used for establishing the primality of the number, declare the primality of the input number.

References

[ABS08] B. Salvy A. Bostan, F. Morain and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77:1755–1778, 2008.

[CHGN08] Don Coppersmith, Nick Howgrave-Graham, and S. V. Nagaraj. Divisors in residue classes, constructively. *Math. Comp.*, 77:531–545, 2008.

[GD67] A. Grothendieck and J. Dieudonné. Eléments de Géométrie Algébrique I-IV. *Inst. Hautes Études Sci. Publ. Math.*, 20, 24, 28, 32, 1960–67.

[Hus04] Dale Husemöller. *Elliptic curves. Second Edition.* Graduate Texts in Mathematics. Springer, 2004.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, 1985.

[Lan90] Serge Lang. *Cyclotomic Fields I and II.* Springer, 1990.

[Len84] Hendrik W. Lenstra, Jr. Divisors in residue classes. *Math. Comp.*, 42:331–340, 1984.

[Mat86] Hideuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1986.

[Mih06a] Preda Mihailescu. Cyclotomic primality proofs and their certificates. arXiv:0709.4112, 2006.

[Mih06b] Preda Mihailescu. Dual elliptic primes and applications to cyclotomic primality proving. 2006 version of arXiv:0709.4113, 2006.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields. Second Edition.* Springer, 1997.

J. Franke, A. Decker: Mathematics institute, Bonn University

T. Kleinjung: LACAL, EPFL Lausanne