Finite Fields and Their Applications 18 (2012) 222–236

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Deterministic primality tests based on tori and elliptic curves

Alexander Gurevich [a], Boris Kunyavskiĭ [b,*]

[a] The Hebrew University of Jerusalem, Givat Ram, 91904 Jerusalem, Israel
[b] Bar-Ilan University, 52900 Ramat Gan, Israel

ARTICLE INFO

Article history:
Received 11 October 2010
Revised 23 March 2011
Accepted 31 July 2011
Available online 7 September 2011
Communicated by Igor Shparlinski

MSC:
11G05
11Y11
14G15
20G35

Keywords:
Group scheme
Elliptic curve
Algebraic torus
Primality test

ABSTRACT

We develop a general framework for producing deterministic primality tests based on commutative group schemes over rings of integers. Our focus is on the cases of algebraic tori and elliptic curves. The proposed general machinery provides several series of tests which include, as special cases, tests discovered by Gross and by Denomme and Savin for Mersenne and Fermat primes, primes of the form $2^{2^{l+1}} - 2^l + 1$, as well as some new ones.

1. Introduction

We propose several deterministic primality tests which involve various group schemes such as tori and elliptic curves and fit into the frame of a general test. Under a deterministic test we mean an explicitly computable necessary and sufficient condition on an element of an infinite set of positive integers which guarantees its primality. We stress that our conditions do not contain a requirement of existence of a group scheme or a point on it with certain properties. Such primality tests are not really deterministic because usually there is no explicit procedure that would provide a group scheme

* Corresponding author.
E-mail addresses: gurevich@math.huji.ac.il (A. Gurevich), kunyav@macs.biu.ac.il (B. Kunyavskiĭ).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.07.011

or a point required. The conditions in our tests always consist in divisibility of a certain element in an explicitly defined recursive sequence by a tested number. This reminds the first primality tests invented by Lucas and Pepin in the 19th century. From the modern point of view, these tests are based on the squaring of a point on an algebraic torus. Recently, several deterministic primality tests involving elliptic curves were discovered by Gross [1] and Denomme and Savin [2].

We are not going to review vast literature concerning primality testing. We would only like to emphasize the importance of revealing connections of many recent innovations with classical works (see [3] for a detailed historical survey and [4] for an excellent description of advanced methods of elliptic curve primality proving (ECPP) and their ties with naive approaches going back to the 19th century). A comprehensive survey of methods of primality proving (with emphasis on computational aspects) can be found, e.g., in [5].

In the present note, our modest goal is to unify the aforementioned deterministic tests within a general framework of group schemes and develop some new ones for families of numbers which were not considered earlier.

We keep following the approach presented in our previous article [6] where we introduced a procedure providing deterministic primality tests based on algebraic groups and showed that Pepin's test and the tests of Lucas–Lehmer type can be viewed as a special case of our construction. In the present paper, we modify and extend this procedure (Section 3) which allows us to shorten the proofs of the toric tests for the numbers of the form $h2^n \pm 1$ (Sections 4 and 5) and include several elliptic tests for the same numbers (Sections 6 and 7). Moreover, we develop elliptic tests for the numbers of the form $g^2 2^{2n-1} - g2^n + 1$ (Section 7) and of the form $g^2 2^{2n} - g2^n + 1$ (Section 8) which, as far as we know, cannot be tested with a toric test.

In Section 6, we apply the general test to an elliptic curve given by the equation $y^2 = x^3 - dx$, where d is not a square modulo the numbers tested for primality. If, in addition, a tested number is prime and congruent to -1 modulo 4, then according to a result of Schoof [7] the groups of points of the corresponding reduced elliptic curve must be cyclic. Thus we obtain an elliptic test for the numbers of the form $h2^n - 1$ which contains Gross' elliptic test for Mersenne numbers [1] as a special case.

Further we consider sets of tested numbers with the property that for any possible prime divisor of a tested number, the corresponding group of points admits a structure of a module over the ring of integers in a quadratic extension of $\mathbb{Q}$. This allows us to obtain a large variety of sets of tested numbers even if the group of points is not cyclic. In Section 7, the general test is applied to the same elliptic curve as in Section 6, but under the assumption that d is a fourth power modulo the tested numbers. In this way we construct primality tests for two families of numbers. The first consists of the numbers of the form $g^2 2^{2n} + 1$. Taking $g = 1$ in this test provides a slight variation of the test introduced by Denomme and Savin [2] for Fermat numbers. The second family consists of the numbers of the form $g^2 2^{2n-1} - g2^n + 1$. In the case where $g = (-1)^{n(n-1)/2}$ we get so-called Gauss–Mersenne norms. In [8], Chudnovsky brothers suggested to use elliptic curves for checking primality of these numbers. However, they did not formulate any deterministic test for them. In Section 8, we develop a test for the numbers of the form $g^2 2^{2n} - g2^n + 1$ applying the general test to an elliptic curve given by the equation $y^2 = x^3 + e^3$ where e is not a square modulo the tested numbers. This test contains the test for the numbers of the form $2^{2^{l+1}} - 2^{2^l} + 1$ described in [2] as a special case.

2. Preliminaries

The initial point of our considerations is the well-known Pocklington test in the case where the factored part of $m - 1$ is a power of 2. It can be formulated as follows.

Pocklington test. *(See [9, Theorems 4.13 and 4.14].) Let m, n, h be positive integers such that $m - 1 = 2^n h$. If there exists a positive integer β such that $\beta^{2^{n-1}h} + 1 \equiv 0 \pmod m$ and $\sqrt{m} \leqslant 2^n$, then m is prime.*

Proof. For any odd prime divisor p of m we have $p \mid \beta^{2^{n-1}h} + 1$, hence $p \mid \beta^{2^n h} - 1$ and $p \nmid \beta^{2^{n-1}h} - 1$. Thus $\alpha = \beta^h$ is of order 2^n in $\mathbb{F}_p^*$, and therefore $2^n \mid p - 1$. Since $\sqrt{m} \leqslant 2^n < p$, we conclude that m is prime. □

There were several attempts to generalize Pocklington's test to arbitrary group schemes, among them [10,11,6]. A Pocklington-type test proposed in the present paper differs from previous generalizations. Namely, we take into account that the order of the group of points of a group scheme can be estimated from below by the order of one of the points better than through Lagrange's theorem. This happens in the case of elliptic curves with complex multiplication.

Let G be a group scheme over $\mathbb{Z}$. For every positive integer m we have the reduction morphism $r_m : G(\mathbb{Z}) \to G(\mathbb{Z}/m\mathbb{Z})$. Moreover, for every $m_1, m_2, m_2 \mid m_1$, we have $r_{m_1,m_2} : G(\mathbb{Z}/m_1\mathbb{Z}) \to G(\mathbb{Z}/m_2\mathbb{Z})$. It is usually easy to find a function f on G whose zeros on $G(\mathbb{F}_p)$ are precisely the elements of order 2 for every prime p.

Suppose that we have an increasing function $\psi : \mathbb{R}^+ \to \mathbb{R}^+$ which estimates the size of $G(\mathbb{F}_p)$ from above, i.e., $\#G(\mathbb{F}_p) \leqslant \psi(p)$ for every prime p, and a function $\rho : \mathbb{R}^+ \to \mathbb{R}^+$ which estimates the size of $G(\mathbb{F}_p)$ from below through the order of its elements, i.e., if in $G(\mathbb{F}_p)$ there is an element of order 2^n, then $\rho(2^n) \leqslant \#G(\mathbb{F}_p)$ for every prime p and integer n. Then we obtain the following

Pocklington-type test. *Let m be a positive integer. If there exists $\alpha \in G(\mathbb{Z}/m\mathbb{Z})$ such that $\alpha^{2^{n-1}}(f) = 0$ and $\psi(\sqrt{m}) < \rho(2^n)$, then m is prime.*

Proof. For any prime divisor p of m we have $r_{m,p}(\alpha^{2^{n-1}})(f) = 0$ which implies that $r_{m,p}(\alpha^{2^{n-1}})$ is of order 2 in $G(\mathbb{F}_p)$. Therefore $r_{m,p}(\alpha)$ is of order 2^n, and hence $\rho(2^n) \leqslant \#G(\mathbb{F}_p) \leqslant \psi(p)$. Since $\psi(\sqrt{m}) < \rho(2^n)$ and ψ is increasing, we get $\sqrt{m} < p$. Thus m must be prime. □

This is a sufficient test which can prove primality of primes p such that $G(\mathbb{F}_p)$ contains an element whose order is a large power of 2. It turns out that restricting the set of tested numbers we can convert it into a deterministic primality test in the sense explained in the Introduction.

We introduce a set M of positive integers tested for primality and a function ξ on M whose values are integer powers of 2 such that $\psi(\sqrt{m}) < \rho(\xi(m))$ for every $m \in M$. Further, we suppose that there exists $\alpha \in G(\mathbb{Z})$ such that for every prime $p \in M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to $\xi(p)$. Then we obtain the following

Deterministic test. *Let $m \in M$. Then m is prime if and only if*

$$r_m\big(\alpha^{\xi(m)/2}\big)(f) = 0.$$

Proof. The "only if" part immediately follows from our assumptions on ξ and α. The "if" part is precisely the Pocklington-type test formulated above. □

Notice that unlike most authors, we require the existence of $\alpha \in G(\mathbb{Z})$ which does not depend on $m \in M$. Thus applying Deterministic test we do not have to search for a suitable α for each element of M. Rather, we can test all elements of M with the aid of the same recurrent sequence.

We are going to derive from Deterministic test some classical tests for the numbers of the form $h2^n \pm 1$, several elliptic tests for the same numbers and also some tests for the numbers of the forms $g^2 2^{2n-1} - g2^n + 1$ and $g^2 2^{2n} - g2^n + 1$. However, the formulation of Deterministic test presented above has two essential drawbacks. First, this test cannot be applied to the multiplicative group scheme since $\mathbb{Z}^*$ contains only two elements: 1 and -1. To circumvent this difficulty, we introduce a finite set S of "bad" primes and assume that G is defined over $\mathbb{Z}_S$ and that no element of M is divisible by an element of S. Second, in the case where G is not affine, the function f cannot be defined on G but only on an open subset U of G. In this case we have to impose an additional requirement that $\alpha \in U(\mathbb{Z}_S)$. In the next section, we describe a precise construction of our deterministic general test.

3. General test

We start with formulating a general deterministic primality test which is a modification of the test introduced in [6].

Let $\mathbb{P}$ denote the set of prime positive integers. We fix an infinite set M of positive integer numbers tested for primality. Usually M is defined as the image of an explicit function of a positive integer argument. We also introduce a finite set $S \subset \mathbb{P}$ which contains 2 and assume that

$(*)$ $s \nmid m$ for any $s \in S$, $m \in M$.

We consider the ring $\mathbb{Z}_S = \{n_1/n_2 \in \mathbb{Q} \mid n_1, n_2 \in \mathbb{Z}, p \nmid n_2 \text{ for any } p \in \mathbb{P} \setminus S\}$ and remind that the points of $\operatorname{Spec}\mathbb{Z}_S$ correspond to the elements of $\mathbb{P} \setminus S \cup \{0\}$ which are the generators of the prime ideals in $\mathbb{Z}_S$.

We say that G is a scheme over $\mathbb{Z}_S$ if G is a scheme together with a morphism $\iota : G \to \operatorname{Spec}\mathbb{Z}_S$. Let A be a $\mathbb{Z}_S$-algebra. An A-point of G is a morphism $\alpha : \operatorname{Spec} A \to G$ such that $\iota \circ \alpha$ corresponds to the structure morphism of A. In particular, if $A = \mathbb{Z}_S$, then a $\mathbb{Z}_S$-point on G is a section of ι. The set of all A-points on G is denoted by $G(A)$. Any homomorphism $A_1 \to A_2$ of $\mathbb{Z}_S$-algebras induces a map $G(A_1) \to G(A_2)$. Thus G provides a functor from the category of $\mathbb{Z}_S$-algebras to the category of sets. If G is, in addition, a group scheme, then $G(A)$ has a group structure for any A, and the map $G(A_1) \to G(A_2)$ is a group homomorphism for any $A_1 \to A_2$. If m is such that $s \nmid m$ for any $s \in S$, then $\mathbb{Z}_S/m\mathbb{Z}_S \cong \mathbb{Z}/m\mathbb{Z}$, and thus we have the reduction map $\mathbb{Z}_S \to \mathbb{Z}/m\mathbb{Z}$. Denote by $r_m : G(\mathbb{Z}_S) \to G(\mathbb{Z}/m\mathbb{Z})$ the corresponding morphism of groups of points.

Let U be an open affine subscheme of G. Then $U \cong \operatorname{Spec} H$ for some $\mathbb{Z}_S$-algebra H. We say that an A-point α of G belongs to U if $\alpha(\operatorname{Spec} A) \subset U$. In this case, α defines a $\mathbb{Z}_S$-homomorphism $H \to A$. For any function $f \in H$ on U, one can define the value of f at α as $\alpha(f)$. If, for instance, $H = \mathbb{Z}_S[x, y]/\mathcal{P}$, where $\mathcal{P} \in \mathbb{Z}_S[x, y]$, then an A-point α of U is defined by $\alpha(x), \alpha(y) \in A$ which satisfy $\mathcal{P}(\alpha(x), \alpha(y)) = 0$. If, in addition, $f \in H$, then $\alpha(f) = f(\alpha(x), \alpha(y))$.

Suppose that we have a group scheme G over $\mathbb{Z}_S$, an open affine subscheme $U = \operatorname{Spec} H$ of G, a function $f \in H$ on U, an increasing function $\psi : \mathbb{R}^+ \to \mathbb{R}^+$, a function $\rho : \{2^l \mid l \in \mathbb{Z}\} \to \mathbb{R}^+$, a $\mathbb{Z}_S$-point α of U, and a function $\xi : M \to \{2^l \mid l \in \mathbb{Z}\}$ such that the following assumptions are satisfied:

(i) for every $p \in \mathbb{P} \setminus S$, $\eta \in G(\mathbb{F}_p)$, the order of η is equal to 2 if and only if η belongs to U and $\eta(f) = 0$;
(ii) for every $p \in \mathbb{P} \setminus S$, we have $\#G(\mathbb{F}_p) \leqslant \psi(p)$;
(iii) for every $p \in \mathbb{P}$, $m \in M$, $l \in \mathbb{Z}$, if $p \mid m$ and in $G(\mathbb{F}_p)$ there is an element of order 2^l, then $\rho(2^l) \leqslant \#G(\mathbb{F}_p)$;
(iv) for every $p \in \mathbb{P} \cap M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to $\xi(p)$;
(v) for every $m \in M$, we have $\psi(\sqrt{m}) < \rho(\xi(m))$.

Notice that if $\rho(x) = x$, then assumption (iii) is automatically satisfied according to Lagrange's theorem.

Then we can formulate the following primality test.

Theorem 1. *Let G, U, f, ψ, ρ, α, ξ be as above. Then $m \in M$ is prime if and only if $r_m(\alpha^{\xi(m)/2}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{\xi(m)/2})(f) = 0$.*

Proof. If $m \in \mathbb{P}$, then according to (iv), the order of $r_m(\alpha)$ in $G(\mathbb{F}_m)$ is $\xi(m)$. Hence the order of $r_m(\alpha^{\xi(m)/2})$ in $G(\mathbb{F}_m)$ is 2, and according to (i), $r_m(\alpha^{\xi(m)/2}) \in U(\mathbb{F}_m)$ and $r_m(\alpha^{\xi(m)/2})(f) = 0$. Conversely, suppose that $r_m(\alpha^{\xi(m)/2}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{\xi(m)/2})(f) = 0$. Let p be the smallest prime divisor of m. Then $r_p(\alpha^{\xi(m)/2}) \in U(\mathbb{F}_p)$ and $r_p(\alpha^{\xi(m)/2})(f) = 0$, and according to (i), the order of $r_p(\alpha^{\xi(m)/2})$ in $G(\mathbb{F}_p)$ is 2. Therefore the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is $\xi(m)$. Now (v), (iii) and (ii) imply $\psi(\sqrt{m}) < \rho(\xi(m)) \leqslant \#G(\mathbb{F}_p) \leqslant \psi(p)$. Since ψ is an increasing function, we get $\sqrt{m} < p$. Thus m must be prime. □

In the next sections, we apply Theorem 1 to various group schemes and the corresponding sets of tested numbers. All sections are organized by the same pattern as follows. First, we fix a certain form of the numbers in question ($h2^n + 1$ in Section 4, $h2^n - 1$ in Sections 5 and 6, $g^2 2^{2n} + 1$ and

$g^2 2^{2n-1} - g2^n + 1$ in Section 7, $g^2 2^{2n-1} - g2^n + 1$ in Section 8) and an appropriate group scheme (the multiplicative group scheme in Section 4, a model of a torus given by $y^2 = dx^2 + x$ in Sections 5, an elliptic curve given by $y^2 = x^3 - dx$ in Sections 6 and 7, an elliptic curve given by $y^2 = x^3 + d$ in Section 8). Then the choice of functions f and ψ is straightforward ($f = 1 + x$, $\psi(x) = x - 1$ in Section 4, $f = 1 + dx$, $\psi(x) = x + 1$ in Sections 5, $f = x^3 - dx$, $\psi(x) = (\sqrt{x} + 1)^2$ in Sections 6 and 7, $f = x^3 + d$, $\psi(x) = (\sqrt{x} + 1)^2$ in Section 8). Also, the choice of ρ is natural ($\rho(x) = x$ in Sections 4, 5 and 6, $\rho(x) = x^2/2$ in Section 7, $\rho(x) = x^2$ in Section 8).

The most complicated is the choice of α. Usually, it is not possible to choose α allowing one to test all numbers of the form under consideration. However, we can find α which suits the numbers of the corresponding form so that h (or g) and n would satisfy certain congruences. Thus we obtain a set M of tested numbers. In order to construct a pair (α, M) satisfying assumptions (iv) and (v), we have to ensure that $r_p(\alpha)$ is not a square in $G(\mathbb{F}_p)$ for any prime $p \in M$. For this purpose we fix a prime z (or two primes z and t) which is not a square modulo any prime from M. This condition gives the restrictions on h (or g) and n mentioned above. Further, we introduce an equation whose rational solution allows one to define $\alpha \in G(\mathbb{Q})$ with the required property ($\kappa u^2 + \mu = \lambda z v^2$ in Sections 5 and 6, $\kappa u^2 + \mu^2 t = \lambda^2 z v^4$ in Section 7, $\lambda^2 v^4 - 3\lambda v^2 + 3 = z$ in Section 8). We do not discuss how to solve these equations in general, but for each of them we give a list of solutions for small values of z (or z and t). For instance, the equation $\kappa u^2 + \mu = \lambda z v^2$ is similar to Pell's equation, and its solution can be obtained by expanding certain quadratic irrationals in continuous fractions. The last step is to fix the set S of "bad" primes so that $\alpha \in G(\mathbb{Z}_S)$. Usually S must contain 2, z (or z and t) and, sometimes, the prime divisors of the denominators of the solutions of the equations mentioned above. In Section 8, S must contain 3.

Finally, we would like to stress that we avoid discussing the question how for a given number of one of the forms under consideration, to find z so that the number would belong to the set of tested numbers corresponding to z. The reason is that we do not have any suggestion but to check all primes successively until we find an appropriate z. Although such z can usually be found very fast, we cannot consider this procedure as deterministic, and therefore the tests for the sets of all numbers of any of the forms introduced above cannot be called deterministic in strict algorithmic sense.

4. Toric tests for $m = h2^n + 1$

Fix an odd positive integer h and suppose that $M \subset \{h2^n + 1 \mid n \geqslant 1,\ h < 2^n\}$. We are going to check primality of the elements of M with the aid of the multiplicative group scheme $G = \operatorname{Spec} \mathbb{Z}_S[x, x^{-1}]$ with the unit $x \mapsto 1$ and the multiplication $x \mapsto x \otimes x$. Let $p \in \mathbb{P} \setminus S$. Clearly, $\eta \in G(\mathbb{F}_p)$ is of order 2 if and only if $\eta(x) = -1$. Further, $\#G(\mathbb{F}_p) = p - 1$ and the group $G(\mathbb{F}_p)$ is cyclic. Finally, if $\gamma \in G(\mathbb{Z}_S)$ and $(\frac{\gamma(x)}{p}) = -1$, then $r_p(\gamma)$ is not a square in $G(\mathbb{F}_p)$.

Proposition 1. *Let $z \in S$ be such that $(\frac{z}{p}) = -1$ for any $p \in \mathbb{P} \cap M$. Then setting $\beta(x) = z$ defines a point $\beta \in G(\mathbb{Z}_S)$, and for any $p = h2^n + 1 \in \mathbb{P} \cap M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha = \beta^h$.*

Proof. Clearly $G(\mathbb{F}_p) \cong \mathbb{Z}/h2^n\mathbb{Z}$. Since $r_p(\beta)$ is not a square in $G(\mathbb{F}_p)$ and h is odd, $r_p(\alpha)$ is not a square either. Thus $r_p(\alpha)$ must be of order 2^n. □

Test 1. *(Cf. [6, Corollary 2.4].) Let z be as in Proposition 1. Then $m = h2^n + 1 \in M$ is prime if and only if $m \mid z^{h2^{n-1}} + 1$.* □

Proof. Take α as in Proposition 1. Then $\alpha^{2^i}(x) = z^{h2^i}$ for any $i \geqslant 0$. Further, take $U = G$, $f = 1 + x$, $\psi(x) = x - 1$, $\rho(x) = x$ and $\xi(h2^n + 1) = 2^n$. Then assumptions (i) and (ii) are obviously satisfied, and according to Proposition 1, assumption (iv) is also satisfied. Finally, assumption (v) follows from $h2^n + 1 < 2^{2n} + 1 < (2^n + 1)^2$. Thus Theorem 1 implies the required statement. □

Example 1. Here are some possible choices of parameters satisfying the hypotheses of Proposition 1 and assumption $(*)$ for three values of z.

Case A: $z=3$, $S=\{2,3\}$.
I) $h\equiv 1 \pmod 6$, $M=\{h2^{2l}+1 \mid l\geqslant 1,\ h<2^{2l}\}$.
II) $h\equiv -1 \pmod 6$, $M=\{h2^{2l+1}+1 \mid l\geqslant 0,\ h<2^{2l+1}\}$.
$m\equiv -1 \pmod 3$ for any $m\in M$, $(\frac{3}{p})=(\frac{p}{3})=-1$ for any $p\in\mathbb{P}\cap M$.
Case B: $z=5$, $S=\{2,5\}$.
I) $h\equiv 1$ or $-3 \pmod{10}$, $M=\{h2^{4l}+1 \mid l\geqslant 1,\ h<2^{4l}\}$.
II) $h\equiv 1$ or $3 \pmod{10}$, $M=\{h2^{4l+1}+1 \mid l\geqslant 0,\ h<2^{4l+1}\}$.
III) $h\equiv -1$ or $3 \pmod{10}$, $M=\{h2^{4l+2}+1 \mid l\geqslant 0,\ h<2^{4l+2}\}$.
IV) $h\equiv -1$ or $-3 \pmod{10}$, $M=\{h2^{4l+3}+1 \mid l\geqslant 0,\ h<2^{4l+3}\}$.
$m\equiv 2$ or $-2 \pmod 5$ for any $m\in M$, $(\frac{5}{p})=(\frac{p}{5})=-1$ for any $p\in\mathbb{P}\cap M$.
Case C: $z=7$, $S=\{2,7\}$.
I) $h\equiv -3$ or $\pm 5 \pmod{14}$, $M=\{h2^{3l}+1 \mid l\geqslant 1,\ h<2^{3l}\}$.
II) $h\equiv \pm 1$ or $-5 \pmod{14}$, $M=\{h2^{3l+1}+1 \mid l\geqslant 0,\ h<2^{3l+1}\}$.
III) $h\equiv 1$ or $\pm 3 \pmod{14}$, $M=\{h2^{3l+2}+1 \mid l\geqslant 0,\ h<2^{3l+2}\}$.
$m\equiv -1, -2$ or $3 \pmod 7$ for any $m\in M$, $(\frac{7}{p})=(\frac{p}{7})=-1$ for any $p\in\mathbb{P}\cap M$.

Pepin's test for Fermat numbers [9, Theorem 4.1.2] is none other than Test 1 applied to Example 1 in case A-I, $h=1$.

5. Toric tests for $m=h2^n-1$

Fix an odd positive integer h and suppose that $M\subset\{h2^n-1 \mid n\geqslant 3,\ h<2^n-2\}$. Let $d\in\mathbb{Z}$ be a square-free integer. We are going to check primality of the elements of M with the aid of the Waterhouse–Weisfeiler group scheme (see [12, Theorem 3.1]) $G=\operatorname{Spec}\mathbb{Z}_S[x,y]/(y^2-dx^2-x)$ with the unit $x\mapsto 0$, $y\mapsto 0$ and the multiplication

$$x\mapsto x\otimes 1+1\otimes x+2y\otimes y+2dx\otimes x,\qquad y\mapsto y\otimes 1+1\otimes y+2dy\otimes x+2dx\otimes y.$$

Remark 1. We have $\gamma^2(x)=4\gamma(x)(1+d\gamma(x))=4\gamma(y)^2$ for any $\gamma\in G(\mathbb{Z}_S)$.

Lemma 1. *Let $p\in\mathbb{P}\setminus S$, $\eta\in G(\mathbb{F}_p)$. Then η is of order 2 if and only if $\eta(1+dx)=0$.*

Proof. According to Remark 1, $\eta^2(x)=0$ if and only if either $\eta(x)=0$ or $\eta(1+dx)=0$. Since $\eta(x)=0$ implies $\eta(y)=0$, we obtain the required statement. □

Proposition 2. *If $p\in\mathbb{P}\setminus S$, then $\#G(\mathbb{F}_p)=p-(\frac{d}{p})$, and the group $G(\mathbb{F}_p)$ is cyclic.*

Proof. This immediately follows from [12, Proposition 3.2] which states that the special fibre of the group scheme G at p is either the norm torus (if p is inert), or the multiplicative group (if p is split), or the additive group (if p is ramified). □

Lemma 2. *Let $p\in\mathbb{P}\setminus S$, $\gamma\in G(\mathbb{Z}_S)$. If $(\frac{\gamma(x)}{p})=-1$, then $r_p(\gamma)$ is not a square in $G(\mathbb{F}_p)$.*

Proof. It follows immediately from Remark 1. □

Proposition 3. *Let $z\in\mathbb{P}$ be such that $(\frac{z}{p})=-1$ for any $p\in\mathbb{P}\cap M$, and let u, $v\in\mathbb{Z}_S$ be such that*

$$\kappa u^2+\mu=\lambda z v^2,$$

where $\kappa\in\{1,-z\}$, λ, $\mu\in\{1,2\}$. Then setting $\beta(x)=-\kappa v^2/\mu$, $\beta(y)=-\kappa uv/\mu$ defines a point $\beta\in G(\mathbb{Z}_S)$ with $d=\lambda z/\kappa$, and for any $p=h2^n-1\in\mathbb{P}\cap M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha=\beta^h$.

Proof. We have $\beta(y)^2 - d\beta(x)^2 = (\kappa^2 u^2 v^2 - \lambda z \kappa v^4)/\mu^2 = -\kappa\mu v^2/\mu^2 = \beta(x)$, and hence β is a point on G. Furthermore, one can notice that $(\frac{\kappa}{p}) = (\frac{\lambda}{p}) = (\frac{\mu}{p}) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $(\frac{d}{p}) = (\frac{\beta(x)}{p}) = -1$. Then Proposition 2 implies that $G(\mathbb{F}_p) \cong \mathbb{Z}/h2^n\mathbb{Z}$. Further, Lemma 2 implies that $r_p(\beta)$ is not a square in $G(\mathbb{F}_p)$. Since h is odd, $r_p(\alpha)$ is not a square either. Thus $r_p(\alpha)$ must be of order 2^n. □

Test 2. *(Cf. [6, Corollary 3.6].) Let d, α be as in Proposition* 3. *Define a sequence $b_i \in \mathbb{Z}_S$ by $b_0 = \alpha(x)$, $b_{i+1} = 4b_i(1 + db_i)$. Then $m = h2^n - 1 \in M$ is prime if and only if $m \mid 1 + db_{n-1}$.*

Proof. Take $U = G$, $f = 1 + dx$, $\psi(x) = x + 1$, $\rho(x) = x$ and $\xi(h2^n - 1) = 2^n$. Then Lemma 1 implies that assumption (i) is satisfied. Assumption (ii) follows from Proposition 2. According to Proposition 3, assumption (iv) is also satisfied. Finally, assumption (v) follows from $h2^n - 1 < (2^n - 2)2^n < (2^n - 1)^2$. Thus Theorem 1 implies that m is prime if and only if $r_m(\alpha^{2^{n-1}})(1 + dx) = 0$. According to Remark 1, we have $\alpha^{2^i}(x) = b_i$ for any $i \geqslant 0$ which gives the required statement. □

Example 2. Here are some possible choices of parameters satisfying the hypotheses of Proposition 3 and assumption $(*)$ for two values of z.

Case A: $z = 3$, $S = \{2, 3\}$.
1) $\kappa = 1$, $\lambda = 1$, $\mu = 2$, $u = 1$, $v = 1$.
2) $\kappa = 1$, $\lambda = 2$, $\mu = 2$, $u = 2$, $v = 1$.
3) $\kappa = -3$, $\lambda = 2$, $\mu = 1$, $u = 1/3$, $v = 1/3$.
4) $\kappa = -3$, $\lambda = 2$, $\mu = 2$, $u = 2/3$, $v = 1/3$.
I) $h \equiv -1 \pmod 6$, $M = \{h2^{2l} - 1 \mid l \geqslant 2,\ h < 2^{2l} - 2\}$.
II) $h \equiv 1 \pmod 6$, $M = \{h2^{2l+1} - 1 \mid l \geqslant 1,\ h < 2^{2l+1} - 2\}$.
$m \equiv 1 \pmod 3$ for any $m \in M$, $(\frac{3}{p}) = -(\frac{p}{3}) = -1$ for any $p \in \mathbb{P} \cap M$.

Case B: $z = 5$, $S = \{2, 5\}$.
1) $\kappa = 1$, $\lambda = 1$, $\mu = 1$, $u = 2$, $v = 1$.
2) $\kappa = 1$, $\lambda = 2$, $\mu = 1$, $u = 3$, $v = 1$.
3) $\kappa = -5$, $\lambda = 1$, $\mu = 1$, $u = 1/5$, $v = 2/5$.
4) $\kappa = -5$, $\lambda = 1$, $\mu = 2$, $u = 1/5$, $v = 3/5$.
I) $h \equiv -1$ or $3 \pmod{10}$, $M = \{h2^{4l} - 1 \mid l \geqslant 1,\ h < 2^{4l} - 2\}$.
II) $h \equiv -1$ or $-3 \pmod{10}$, $M = \{h2^{4l+1} - 1 \mid l \geqslant 1,\ h < 2^{4l+1} - 2\}$.
III) $h \equiv 1$ or $-3 \pmod{10}$, $M = \{h2^{4l+2} - 1 \mid l \geqslant 1,\ h < 2^{4l+2} - 2\}$.
IV) $h \equiv 1$ or $3 \pmod{10}$, $M = \{h2^{4l+3} - 1 \mid l \geqslant 1,\ h < 2^{4l+3} - 2\}$.
$m \equiv 2$ or $-2 \pmod 5$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$ for any $p \in \mathbb{P} \cap M$.

The classical Lucas–Lehmer test for Mersenne numbers [9, Theorem 4.2.6] can be obtained by applying Test 2 to Example 2 in case A-1-II, $h = 1$, and replacing the sequence b_i by the sequence $a_i = 12b_i + 2$ (see [6, Corollary 3.8]).

6. Elliptic tests for $m = h2^n - 1$

Fix an odd positive integer h and suppose that $M \subset \{h2^n - 1 \mid n \geqslant 3,\ h < 2^n - 2^{(n+4)/2}\}$. Let $d \in \mathbb{Z}_S$, $p \nmid d$ for any $p \in \mathbb{P} \setminus S$. We are going to check primality of the elements of M with the aid of the elliptic curve G given by the equation $y^2 = x^3 - dx$.

Remark 2. We have $\eta^2(x) = \frac{(\eta(x)^2+d)^2}{4(\eta(x)^3 - d\eta(x))} = \frac{(\eta(x)^2+d)^2}{4\eta(y)^2}$ for any $\eta \in G(K)$ different from the identity, where K is a field such that $\operatorname{char} K \notin S$.

Lemma 3. *Let $p \in \mathbb{P} \setminus S$, $\eta \in G(\mathbb{F}_p)$. Then η is of order* 2 *if and only if $\eta(x^3 - dx) = 0$.*

Proof. It follows immediately from Remark 2. □

Proposition 4. *If $p \in \mathbb{P} \setminus S$ and $p \equiv -1 \pmod 4$, then $\#G(\mathbb{F}_p) = p+1$ and either $G(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)\mathbb{Z}$ or $G(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\frac{p+1}{2}\mathbb{Z}$. The second case can only occur if $(\frac{d}{p}) = 1$.*

Proof. According to [13, Theorem 5 in §18.4], we have $\#G(\mathbb{F}_p) = p+1$. Further, [7, Lemma 4.8] implies that either $G(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)\mathbb{Z}$ or $G(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\frac{p+1}{2}\mathbb{Z}$. Finally, if $(\frac{d}{p}) = -1$, then Lemma 3 implies that there is only one element of order 2 in $G(\mathbb{F}_p)$. Thus the second option for $G(\mathbb{F}_p)$ does not occur. □

Lemma 4. *Let $p \in \mathbb{P} \setminus S$, $\gamma \in G(\mathbb{Z}_S)$. If $(\frac{\gamma(x)}{p}) = -1$, then $r_p(\gamma)$ is not a square in $G(\mathbb{F}_p)$.*

Proof. It immediately follows from Remark 2. □

Proposition 5. *Let $z \in S$ be such that $(\frac{z}{p}) = -1$ for any $p \in \mathbb{P} \cap M$. Let $u, v \in \mathbb{Z}_S$ be such that $1/v \in \mathbb{Z}_S$ and*

$$\kappa u^2 + \mu = \lambda z v^2,$$

where $\kappa \in \{1, -z\}$, $\lambda, \mu \in \{1, 2\}$. Then setting $\beta(x) = -\kappa\mu$, $\beta(y) = \kappa^2\mu u$ defines a point $\beta \in G(\mathbb{Z}_S)$ with $d = \lambda\mu\kappa^2 z v^2$, and for any $p = h2^n - 1 \in \mathbb{P} \cap M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha = \beta^h$.

Proof. We have $\beta(x)^3 - d\beta(x) = -\kappa^3\mu^3 + \lambda\mu\kappa^2 z v^2 \kappa\mu = \kappa^3\mu^2(-\mu + \lambda z v^2) = \kappa^3\mu^2\kappa u^2 = \beta(y)^2$, and hence β is a point on G. Furthermore, one can notice that $(\frac{\kappa}{p}) = (\frac{\lambda}{p}) = (\frac{\mu}{p}) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $(\frac{d}{p}) = (\frac{\beta(x)}{p}) = -1$. Then Proposition 4 implies that $G(\mathbb{F}_p) \cong \mathbb{Z}/h2^n\mathbb{Z}$. Further, Lemma 4 implies that $r_p(\beta)$ is not a square in $G(\mathbb{F}_p)$. Since h is odd, $r_p(\alpha)$ is not a square either. Thus $r_p(\alpha)$ must be of order 2^n. □

Test 3. *Let d, α be as in Proposition 5. Define a sequence $b_i \in \mathbb{Z}_S$ by $b_0 = \alpha(x)$, $b_{i+1} = \frac{(b_i^2+d)^2}{4(b_i^3 - db_i)}$. Then $m = h2^n - 1 \in M$ is prime if and only if $(m, b_i^3 - db_i) = 1$ for any $0 \leqslant i \leqslant n-2$ and $m \mid b_{n-1}^3 - db_{n-1}$.*

Proof. Let $U = \operatorname{Spec} \mathbb{Z}_S[x, y]/(y^2 - x^3 + dx)$ be the standard affine chart of G. Take $f = x^3 - dx$, $\psi(x) = (\sqrt{x}+1)^2$, $\rho(x) = x$ and $\xi(h2^n - 1) = 2^n$. Then Lemma 3 implies that assumption (i) is satisfied. Assumption (ii) follows from Hasse's theorem. According to Proposition 5, assumption (iv) is also satisfied. Finally, assumption (v) follows from $h2^n - 1 < (2^{n/2} - 1)^4$ which holds since $h < 2^n - 4\cdot 2^{n/2} + 6 - 4\cdot 2^{-n/2}$. Thus Theorem 1 implies that m is prime if and only if $r_m(\alpha^{2^{n-1}}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{2^{n-1}})(x^3 - dx) = 0$. Now if $m \in \mathbb{P} \cap M$, then $r_m(\alpha^{2^{n-1}}) \in U(\mathbb{Z}/m\mathbb{Z})$ implies $r_m(\alpha^{2^i}) \in U(\mathbb{Z}/m\mathbb{Z})$ for any $1 \leqslant i \leqslant n-1$. Moreover, according to Remark 2, we get $(m, r_m(\alpha^{2^{i-1}})(x^3 - dx)) = 1$ and $r_m(\alpha^{2^i})(x) \equiv b_i \pmod m$ for any $1 \leqslant i \leqslant n-1$. Hence $(m, b_i^3 - db_i) = 1$ for any $0 \leqslant i \leqslant n-2$, and $r_m(\alpha^{2^{n-1}})(x^3 - dx) = 0$ implies $m \mid b_{n-1}^3 - db_{n-1}$. Conversely, if $(m, b_i^3 - db_i) = 1$ for any $0 \leqslant i \leqslant n-2$ and $m \mid b_{n-1}^3 - db_{n-1}$, then $r_m(\alpha^{2^i}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{2^i})(x) \equiv b_i \pmod m$ for any $1 \leqslant i \leqslant n-1$. Therefore $r_m(\alpha^{2^{n-1}})(x^3 - dx) \equiv b_{n-1}^3 - db_{n-1} \equiv 0 \pmod m$. □

The condition $m \mid b_{n-1}^3 - db_{n-1}$ in Test 3 can be replaced by the stronger condition $m \mid b_{n-1}$ since for any $p \in \mathbb{P} \cap M$, $b \in \mathbb{Z}_S$ we have $p \nmid b^2 - d$.

It is remarkable that the hypotheses of Proposition 5 are almost identical to those of Proposition 3 (the only additional requirement is $1/v \in \mathbb{Z}_S$). Thus Test 3 can be applied to all cases in Example 2 except case B-4.

Gross' elliptic test for Mersenne numbers [1, Proposition 2.2] is none other than Test 3 applied to Example 2 in case A-2-II, $h = 1$.

7. Elliptic tests for $m = g^2 2^{2n} + 1$ and $m = g^2 2^{2n-1} - g2^n + 1$

Fix an odd integer g and suppose that $M \subset \{g^2 2^{2n} + 1 \mid n \geqslant 3,\ |g| < 2^{n-1} - 2\}$ (resp. $M \subset \{g^2 2^{2n-1} - g2^n + 1 \mid n \geqslant 3,\ |g| < 2^{n-1/2} - 2\}$). Let $d \in \mathbb{Z}_S$, $p \nmid d$ for any $p \in \mathbb{P} \setminus S$. We are going to check primality of the elements of M with the aid of the elliptic curve G given by the equation $y^2 = x^3 - dx$.

Let $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 4$, $\varepsilon \in \mathbb{F}_p$ be such that $\varepsilon^2 + 1 = 0$. Define a map $i : G(\mathbb{F}_p) \to G(\mathbb{F}_p)$ as follows: $i(x, y) = (-x, \varepsilon y)$. Clearly, i is an endomorphism of $G(\mathbb{F}_p)$, and thus $G(\mathbb{F}_p)$ gets a structure of $\mathbb{Z}[i]$-module.

Remark 3. We have $\eta^{1+i}(x) = \frac{\eta(y)^2}{(1+\varepsilon)^2 \eta(x)^2}$ for any $\eta \in G(\mathbb{F}_p)$ different from the identity, $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 4$.

Lemma 5. *(Cf. [2, Proposition 4].) Let $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 4$, be such that $\#G(\mathbb{F}_p) = h2^n$, $2 \nmid h$. Then $G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^n\mathbb{Z}[i] \oplus H$ as $\mathbb{Z}[i]$-modules, where H is a $\mathbb{Z}[i]$-module, $\#H = h$.*

Proof. Since $G(\mathbb{F}_p)$ is a finitely generated $\mathbb{Z}[i]$-module, it must be isomorphic to $\bigoplus_{l=1}^{k} \mathbb{Z}[i]/\theta_l\mathbb{Z}[i]$, where $\theta_1, \ldots, \theta_k \in \mathbb{Z}[i]$ are powers of primes in $\mathbb{Z}[i]$, and $\#G(\mathbb{F}_p) = \prod_{l=1}^{k} N(\theta_l)$. Since $1+i$ is the only prime in $\mathbb{Z}[i]$ with norm divisible by 2, there exists $0 \leqslant \tilde{k} \leqslant k$ such that θ_l is a power of $1+i$ for any $1 \leqslant l \leqslant \tilde{k}$, and $N(\theta_l)$ is odd for any $\tilde{k} < l \leqslant k$. Put $H = \bigoplus_{l=\tilde{k}+1}^{k} \mathbb{Z}[i]/\theta_l\mathbb{Z}[i]$. Finally, Remark 3 implies that in $G(\mathbb{F}_p)$ viewed as a $\mathbb{Z}[i]$-module, there is precisely one element of order $1+i$. Thus $\tilde{k} = 1$ and $G(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}[i]/(1+i)^n\mathbb{Z}[i] \oplus H$. □

For $m = g^2 2^{2n} + 1 \in M$, define

$$m' = 1 + g2^n i, \tag{1}$$

and for $m = g^2 2^{2n-1} - g2^n + 1 \in M$, define

$$m' = 1 + g(-1)^{n(n-1)/2}(-1+i)^{2n-1}. \tag{2}$$

We have $N(m') = m$ where $N : \mathbb{Q}(i) \to \mathbb{Q}$ denotes the norm map. If $p \in \mathbb{P} \cap M$, then p' must be prime in the ring $\mathbb{Z}[i]$.

Proposition 6. *If $p = g^2 2^{2n} + 1 \in \mathbb{P} \cap M$ (resp. $p = g^2 2^{2n-1} - g2^n + 1 \in \mathbb{P} \cap M$) and $(\frac{d}{p'})_4 = 1$, then $\#G(\mathbb{F}_p) = g^2 2^{2n}$ (resp. $\#G(\mathbb{F}_p) = g^2 2^{2n-1}$) and $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$ (resp. $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^{n-1}\mathbb{Z} \oplus H$) as abelian groups, where H is an abelian group, $\#H = g^2$.*

Proof. Take $a, b \in \mathbb{Z}$ such that $p' = a + bi$. Then $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$ and $p = a^2 + b^2$. Therefore, according to [13, Theorem 5 in §18.4], we get

$$\#G(\mathbb{F}_p) = p + 1 - (a+bi) - (a-bi) = a^2 + b^2 + 1 - 2a = N\big((a-1) + bi\big) = N\big(p' - 1\big).$$

Thus $\#G(\mathbb{F}_p) = g^2 2^{2n}$ (resp. $\#G(\mathbb{F}_p) = g^2 2^{2n-1}$). Finally, Lemma 5 implies

$$G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n}\mathbb{Z}[i] \oplus H \quad \big(\text{resp. } G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n-1}\mathbb{Z}[i] \oplus H\big)$$

as $\mathbb{Z}[i]$-modules. Since 1 and $1+i$ generate $\mathbb{Z}[i]$ as abelian group, we conclude that $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$ (resp. $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^{n-1}\mathbb{Z} \oplus H$) as abelian groups. □

Lemma 6. *Let $m = g^2 2^{2n} + 1$ (resp. $m = g^2 2^{2n-1} - g2^n + 1$), $p \in \mathbb{P}$, $p \mid m$, $\eta \in G(\mathbb{F}_p)$, $l \in \mathbb{Z}$. If the order of η in $G(\mathbb{F}_p)$ is 2^l, then $\#G(\mathbb{F}_p) \geqslant 2^{2l-1}$.*

Proof. The equation $x^2 + 1 \equiv 0 \pmod p$ has a solution. Indeed, if $m = g^2 2^{2n} + 1$, then one can take $x = g2^n$, and if $m = g^2 2^{2n-1} - g2^n + 1$, then one can take $x = g^2 2^{2n-1}$ since $g^2 2^{2n-1} - g2^n + 1$ divides $g^4 2^{4n-2} + 1$. This implies $p \equiv 1 \pmod 4$. Thus $G(\mathbb{F}_p)$ has a $\mathbb{Z}[i]$-module structure. The ideal of $\mathbb{Z}[i]$ which annihilates η must be either $(1+i)^{2l}\mathbb{Z}[i]$ or $(1+i)^{2l-1}\mathbb{Z}[i]$. Then the $\mathbb{Z}[i]$-submodule of $G(\mathbb{F}_p)$ generated by η contains either 2^{2l} or 2^{2l-1} elements. □

Lemma 7. *Let $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 4$, $\gamma \in G(\mathbb{Z}_S)$. If $(\frac{\gamma(x)}{p}) = -1$, then $r_p(\gamma)$ does not belong to the submodule $G(\mathbb{F}_p)^{1+i}$ of $G(\mathbb{F}_p)$.*

Proof. It immediately follows from Remark 3. □

Proposition 7. *Let $z, t \in S$ be such that $(\frac{z}{p}) = -1$, $(\frac{zt}{p}) = 1$ for any $p \in \mathbb{P} \cap M$. Let $u, v, w \in \mathbb{Z}_S$ be such that*

$$\kappa u^2 + 1 = \lambda z v^2, \qquad \kappa u^2 + 2 = \mu t w^2,$$

where $\kappa, \lambda, \mu \in \{1, 2, -1, -2\}$. Then setting $\beta(x) = e\lambda z v^2$, $\beta(y) = e^2 u v w$ defines a point $\beta \in G(\mathbb{Z}_S)$ with $d = e^2$, $e = \kappa\lambda\mu zt$, and for any $p = g^2 2^{2n} + 1 \in \mathbb{P} \cap M$ (resp. $p = g^2 2^{2n-1} - g2^n + 1 \in \mathbb{P} \cap M$), the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha = \beta^{g^2}$.

Proof. We have $\beta(x)^3 - d\beta(x) = e^3\lambda^3 z^3 v^6 - e^3\lambda z v^2 = e^3\lambda z v^2(\lambda^2 z^2 v^4 - 1) = e^3\lambda z v^2(\lambda z v^2 - 1)(\lambda z v^2 + 1) = e^4 u^2 v^2 w^2 = \beta(y)^2$ and hence β is a point on G. Further, one can notice that $(\frac{\kappa}{p}) = (\frac{\lambda}{p}) = (\frac{\mu}{p}) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $(\frac{d}{p'})_4 \equiv d^{\frac{p-1}{4}} = e^{\frac{p-1}{2}} \equiv (\frac{e}{p}) = 1 \pmod{p'}$, $(\frac{\beta(x)}{p}) = -1$, where p' is given by formula (1) (resp. by formula (2)). Then Proposition 6 implies that $\#G(\mathbb{F}_p) = g^2 2^{2n}$ (resp. $\#G(\mathbb{F}_p) = g^2 2^{2n-1}$). Moreover, according to Lemma 5, $G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n}\mathbb{Z}[i] \oplus H$ (resp. $G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n-1}\mathbb{Z}[i] \oplus H$). Further, Lemma 7 implies that $r_p(\beta)$ does not belong to the submodule $G(\mathbb{F}_p)^{1+i}$ of $G(\mathbb{F}_p)$. Since g^2 is odd, $r_p(\alpha)$ does not belong to $G(\mathbb{F}_p)^{1+i}$ either. Hence $r_p(\alpha)^{2^{n-1}} = r_p(\alpha)^{(-i)^{n-1}(1+i)^{2n-2}}$ is different from the identity in $G(\mathbb{F}_p)$. Since $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$ (resp. $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^{n-1}\mathbb{Z} \oplus H$), the order of $r_p(\alpha)$ must be equal to 2^n. □

Proposition 8. *Let $z, t \in S$ be such that $(\frac{z}{p}) = -1$, $(\frac{zt}{p'})_4 = 1$ for any $p \in \mathbb{P} \cap M$ where p' is defined by formula (1) (resp. by formula (2)). Let $u, v \in \mathbb{Z}_S$ be such that*

$$\kappa u^2 + \mu^2 t = \lambda^2 z v^4,$$

where $\kappa, \lambda, \mu \in \{1, 2, -1, -2\}$. Then setting $\beta(x) = \kappa\lambda^2 z v^2$, $\beta(y) = \kappa^2\lambda^2 z u v$ defines a point $\beta \in G(\mathbb{Z}_S)$ with $d = \kappa^2\lambda^2\mu^2 zt$, and for any $p = g^2 2^{2n} + 1 \in \mathbb{P} \cap M$ (resp. $p = g^2 2^{2n-1} - g2^n + 1 \in \mathbb{P} \cap M$), the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha = \beta^{g^2}$.

Proof. We have $\beta(x)^3 - d\beta(x) = \kappa^3\lambda^6 z^3 v^6 - \kappa^3\lambda^4\mu^2 z^2 t v^2 = \kappa^3\lambda^4 z^2 v^2(\lambda^2 z v^4 - \mu^2 t) = \kappa^4\lambda^4 z^2 v^2 u^2 = \beta(y)^2$ and hence β is a point on G. Further, one can notice that $(\frac{\kappa}{p}) = (\frac{\lambda}{p}) = (\frac{\mu}{p}) = 1$ for any $p \in \mathbb{P} \cap M$, and hence, $(\frac{d}{p'})_4 = (\frac{\kappa^2\lambda^2\mu^2}{p'})_4 \equiv (\kappa^2\lambda^2\mu^2)^{\frac{p-1}{4}} = (\kappa\lambda\mu)^{\frac{p-1}{2}} \equiv (\frac{\kappa\lambda\mu}{p}) = 1 \pmod{p'}$, $(\frac{\beta(x)}{p}) = -1$. The end of the proof is identical to that of Proposition 7. □

Test 4. *Let d, α be either as in Proposition 7 or as in Proposition 8. Define a sequence $b_i \in \mathbb{Z}_S$ by $b_0 = \alpha(x)$, $b_{i+1} = \frac{(b_i^2+d)^2}{4(b_i^3 - db_i)}$. Then $m = g^2 2^{2n} + 1 \in M$ (resp. $m = g^2 2^{2n-1} - g2^n + 1 \in M$) is prime if and only if $(m, b_i^3 - db_i) = 1$ for any $0 \leqslant i \leqslant n-2$ and $m \mid b_{n-1}^3 - db_{n-1}$.*

Proof. Let $U = \operatorname{Spec}\mathbb{Z}_S[x, y]/(y^2 - x^3 + dx)$ be the standard affine chart of G. Take $f = x^3 - dx$, $\psi(x) = (\sqrt{x}+1)^2$, $\rho(x) = x^2/2$ and $\xi(g^2 2^{2n} + 1) = 2^n$ (resp. $\xi(g^2 2^{2n-1} - g2^n + 1) = 2^n$). Then Lemma 3 implies that assumption (i) is satisfied. Assumption (ii) follows from Hasse's theorem. Lemma 6 implies that assumption (iii) is satisfied. According to Propositions 7 and 8 assumption (iv) is also satisfied. Finally, assumption (v) follows from $g^2 2^{2n} + 1 < (2^{(2n-1)/2} - 1)^4$ (resp. $g^2 2^{2n-1} + |g|2^n + 1 < (2^{(2n-1)/2} - 1)^4$) which holds for any $n \geqslant 3$, since

$$g^2 < 2^{2n-2} - 4 \cdot 2^{n-1} + 4 < 2^{2n-2} - 4 \cdot 2^{(2n-3)/2}$$
$$\big(\text{resp. } g^2 < 2^{2n-1} - 4 \cdot 2^{(2n-1)/2} + 4 \text{ and } |g| < 2^n - 2^{3/2}\big).$$

Thus Theorem 1 implies that m is prime if and only if $r_m(\alpha^{2^{n-1}}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{2^{n-1}})(x^3 - dx) = 0$. The end of the proof is identical to that of Test 3. □

If $m = g^2 2^{2n} + 1$ (resp. $m = g^2 2^{2n-1} - g2^n + 1$), then the condition $m \mid b_{n-1}^3 - db_{n-1}$ in Test 4 can be replaced by the stronger condition $m \mid b_{n-1}^2 - d$ (resp. $m \mid b_{n-1}$). Indeed, for any $p \in \mathbb{P} \cap M$, Lemma 7 implies that $r_p(\alpha)$ does not belong to $G(\mathbb{F}_p)^{1+i}$. Then according to Proposition 6 the element $r_p(\alpha^{2^{n-1}})^{1+i} = r_p(\alpha)^{(-i)^{n-1}(1+i)^{2n-1}}$ is different from (resp. equal to) the identity in $G(\mathbb{F}_p)$. Hence by Remark 3 we obtain $r_p(\alpha^{2^{n-1}})(x) \neq 0$ (resp. $r_p(\alpha^{2^{n-1}})(x) = 0$).

Example 3. Here are some possible choices of parameters satisfying the hypotheses of Proposition 7 and assumption $(*)$ for three pairs of values of z, t.

Case A: $z = 5$, $t = 3$, $S = \{2, 3, 5\}$, $\kappa = 1$, $\lambda = 1$, $\mu = 2$, $u = 2$, $v = 1$, $w = 1$, $d = 900$, $\beta(x) = 150$, $\beta(y) = 1800$.
I) $g \equiv \pm 1$ or $\pm 11 \pmod{30}$, $M = \{g^2 2^{4l} + 1 \mid l \geqslant 2,\ g < 2^{2l-1} - 2\}$.
II) $g \equiv \pm 7$ or $\pm 13 \pmod{30}$, $M = \{g^2 2^{4l+2} + 1 \mid l \geqslant 1,\ g < 2^{2l} - 2\}$.
III) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l-1} - g2^{4l} + 1 \mid l \geqslant 1,\ g < 2^{4l-1/2}\}$.
IV) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+1} - g2^{4l+1} + 1 \mid l \geqslant 1,\ g < 2^{4l+1/2}\}$.
V) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+3} - g2^{4l+2} + 1 \mid l \geqslant 1,\ g < 2^{4l+3/2}\}$.
VI) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+5} - g2^{4l+3} + 1 \mid l \geqslant 0,\ g < 2^{4l+5/2}\}$.
$m \equiv 2$ or $-2 \pmod 5$, $m \equiv -1 \pmod 3$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{3}{p}) = (\frac{p}{3}) = -1$ for any $p \in \mathbb{P} \cap M$.

Case B: $z = 7$, $t = 3$, $S = \{2, 3, 7\}$, $\kappa = -2$, $\lambda = -1$, $\mu = -2$, $u = 2$, $v = 1$, $w = 1$, $d = 7056$, $\beta(x) = 588$, $\beta(y) = 14112$.
I) $g \equiv \pm 5, \pm 11, \pm 17$ or $\pm 19 \pmod{42}$, $M = \{g^2 2^{6l} + 1 \mid l \geqslant 1,\ g < 2^{3l-1} - 2\}$.
II) $g \equiv \pm 1, \pm 5, \pm 13$ or $\pm 19 \pmod{42}$, $M = \{g^2 2^{6l+2} + 1 \mid l \geqslant 1,\ g < 2^{3l} - 2\}$.
III) $g \equiv \pm 1, \pm 11, \pm 13$ or $\pm 17 \pmod{42}$, $M = \{g^2 2^{6l+4} + 1 \mid l \geqslant 1,\ g < 2^{3l+1} - 2\}$.
IV) $g \equiv -11, 13$ or $19 \pmod{42}$, $M = \{g^2 2^{4l-1} - g2^{2l} + 1 \mid l \geqslant 2,\ g < 2^{2l-1/2} - 2\}$.
V) $g \equiv -1, 5$ or $17 \pmod{42}$, $M = \{g^2 2^{4l+1} - g2^{2l+1} + 1 \mid l \geqslant 1,\ g < 2^{2l+1/2} - 2\}$.
$m \equiv -1, -2$ or $3 \pmod 7$, $m \equiv -1 \pmod 3$ for any $m \in M$, $(\frac{7}{p}) = (\frac{p}{7}) = -1$, $(\frac{3}{p}) = (\frac{p}{3}) = -1$ for any $p \in \mathbb{P} \cap M$.

Case C: $z = 5$, $t = 7$, $S = \{2, 3, 5, 7\}$, $\kappa = -1$, $\lambda = 1$, $\mu = 2$, $u = 2/3$, $v = 1/3$, $w = 1/3$, $d = 4900$, $\beta(x) = -350/9$, $\beta(y) = 9800/27$.
I) $g \equiv \pm 9, \pm 11, \pm 19$ or $\pm 31 \pmod{70}$, $M = \{g^2 2^{12l} + 1 \mid l \geqslant 2,\ g < 2^{6l-1} - 2\}$.
II) $g \equiv \pm 3, \pm 13, \pm 17$ or $\pm 27 \pmod{70}$, $M = \{g^2 2^{12l+2} + 1 \mid l \geqslant 2,\ g < 2^{6l} - 2\}$.
III) $g \equiv \pm 1, \pm 9, \pm 19$ or $\pm 29 \pmod{70}$, $M = \{g^2 2^{12l+4} + 1 \mid l \geqslant 2,\ g < 2^{6l+1} - 2\}$.
IV) $g \equiv \pm 3, \pm 17, \pm 23$ or $\pm 33 \pmod{70}$, $M = \{g^2 2^{12l+6} + 1 \mid l \geqslant 2,\ g < 2^{6l+2} - 2\}$.
V) $g \equiv \pm 1, \pm 11, \pm 29$ or $\pm 31 \pmod{70}$, $M = \{g^2 2^{12l+8} + 1 \mid l \geqslant 2,\ g < 2^{6l+3} - 2\}$.
VI) $g \equiv \pm 13, \pm 23, \pm 27$ or $\pm 33 \pmod{70}$, $M = \{g^2 2^{12l+10} + 1 \mid l \geqslant 2,\ g < 2^{6l+4} - 2\}$.
VII) $g \equiv -9, -29$ or $31 \pmod{70}$, $M = \{g^2 2^{8l-1} - g2^{4l} + 1 \mid l \geqslant 1,\ g < 2^{4l-1/2} - 2\}$.
VIII) $g \equiv 3, 13$ or $33 \pmod{70}$, $M = \{g^2 2^{8l+1} - g2^{4l+1} + 1 \mid l \geqslant 1,\ g < 2^{4l+1/2} - 2\}$.
IX) $g \equiv -1, -11$ or $19 \pmod{70}$, $M = \{g^2 2^{8l+3} - g2^{4l+2} + 1 \mid l \geqslant 1,\ g < 2^{4l+3/2} - 2\}$.

X) $g \equiv 17, -23$ or $27 \pmod{70}$, $M = \{g^2 2^{8l+5} - g2^{4l+3} + 1 \mid l \geqslant 1,\ g < 2^{4l+5/2} - 2\}$.
$m \equiv 2$ or $-2 \pmod 5$, $m \equiv -1, -2$ or $3 \pmod 7$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{7}{p}) = (\frac{p}{7}) = -1$ for any $p \in \mathbb{P} \cap M$.

For any $p \in \mathbb{P} \cap M$ we have $(\frac{-1}{p'})_4 \equiv (-1)^{\frac{p-1}{4}} = 1 \pmod{p'}$. Besides, if $p' = a + bi$ with $a, b \in \mathbb{Z}$, then $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, and for any odd $q \in \mathbb{Z}$ we have $(-1)^{(q-1)/2} q \equiv 1 \pmod 4$. Thus the biquadratic reciprocity law [13, Theorem 2 in §9.9] implies $(\frac{q}{p'})_4 = (\frac{(-1)^{(q-1)/2} q}{p'})_4 = (\frac{p'}{q})_4$.

Example 4. Here are some possible choices of parameters satisfying the hypotheses of Proposition 8 and assumption $(*)$ for five pairs of values of z, t.

Case A: $z = 5$, $t = 3$, $S = \{2, 3, 5\}$, $\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 1$, $v = 1$, $d = 60$, $\beta(x) = 10$, $\beta(y) = 20$.
I) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l} + 1 \mid l \geqslant 1,\ g < 2^{4l-1} - 2\}$.
II) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+2} + 1 \mid l \geqslant 1,\ g < 2^{4l} - 2\}$.
III) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+4} + 1 \mid l \geqslant 1,\ g < 2^{4l+1} - 2\}$.
IV) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+6} + 1 \mid l \geqslant 0,\ g < 2^{4l+2} - 2\}$.
$m \equiv 2 \pmod 5$, $m' \equiv -1 \pmod{2+i}$, $m' \equiv -i \pmod{2-i}$, $m' \equiv 1 + i \pmod 3$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{15}{p'})_4 = (\frac{p'}{(2+i)\cdot(2-i)\cdot 3})_4 = (-1) \cdot (-i) \cdot (-i) = 1$ for any $p \in \mathbb{P} \cap M$.
V) $g \equiv -1 \pmod{30}$, $M = \{g^2 2^{8l} + 1 \mid l \geqslant 1,\ g < 2^{4l-1} - 2\}$.
VI) $g \equiv 7 \pmod{30}$, $M = \{g^2 2^{8l+2} + 1 \mid l \geqslant 1,\ g < 2^{4l} - 2\}$.
VII) $g \equiv 11 \pmod{30}$, $M = \{g^2 2^{8l+4} + 1 \mid l \geqslant 1,\ g < 2^{4l+1} - 2\}$.
VIII) $g \equiv 13 \pmod{30}$, $M = \{g^2 2^{8l+6} + 1 \mid l \geqslant 0,\ g < 2^{4l+2} - 2\}$.
$m \equiv 2 \pmod 5$, $m' \equiv i \pmod{2+i}$, $m' \equiv -1 \pmod{2-i}$, $m' \equiv 1 - i \pmod 3$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{15}{p'})_4 = (\frac{p'}{(2+i)\cdot(2-i)\cdot 3})_4 = i \cdot (-1) \cdot i = 1$ for any $p \in \mathbb{P} \cap M$.
IX) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l-1} - g2^{4l} + 1 \mid l \geqslant 1,\ g < 2^{4l-1/2}\}$.
X) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+3} - g2^{4l+2} + 1 \mid l \geqslant 1,\ g < 2^{4l+3/2}\}$.
$m \equiv -2 \pmod 5$, $m' \equiv -1 \pmod{2+i}$, $m' \equiv i \pmod{2-i}$, $m' \equiv -1 + i \pmod 3$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{15}{p'})_4 = (\frac{p'}{(2+i)\cdot(2-i)\cdot 3})_4 = (-1) \cdot i \cdot i = 1$ for any $p \in \mathbb{P} \cap M$.
XI) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+1} - g2^{4l+1} + 1 \mid l \geqslant 1,\ g < 2^{4l+1/2}\}$.
XII) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+5} - g2^{4l+3} + 1 \mid l \geqslant 0,\ g < 2^{4l+5/2}\}$.
$m \equiv -2 \pmod 5$, $m' \equiv -i \pmod{2+i}$, $m' \equiv -1 \pmod{2-i}$, $m' \equiv -1 - i \pmod 3$ for any $m \in M$, $(\frac{5}{p}) = (\frac{p}{5}) = -1$, $(\frac{15}{p'})_4 = (\frac{p'}{(2+i)\cdot(2-i)\cdot 3})_4 = (-i) \cdot (-1) \cdot (-i) = 1$ for any $p \in \mathbb{P} \cap M$.

Case B: $z = 7$, $t = 3$, $S = \{2, 3, 7\}$, $\kappa = 1$, $\lambda = 1$, $\mu = 1$, $u = 2$, $v = 1$, $d = 21$, $\beta(x) = 7$, $\beta(y) = 14$.

Case C: $z = 7$, $t = 5$, $S = \{2, 5, 7\}$, $\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 1$, $v = 1$, $d = 140$, $\beta(x) = 14$, $\beta(y) = 28$.

Case D: $z = 3$, $t = 13$, $S = \{2, 3, 7\}$, $\kappa = -1$, $\lambda = 2$, $\mu = 1$, $u = 1$, $v = 1$, $d = 156$, $\beta(x) = -12$, $\beta(y) = 12$.

Case E: $z = 13$, $t = 5$, $S = \{2, 5, 13\}$, $\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 2$, $v = 1$, $d = 260$, $\beta(x) = 26$, $\beta(y) = 104$.

The test by Denomme and Savin for Fermat numbers [2, Theorem in §4] is similar to the test which can be obtained by applying Test 4 to Example 3 in case A-I, $g = 1$, and replacing the sequence b_i by the sequence $a_i = b_i/30$.

If $m = g^2 2^{2n-1} - g2^n + 1$ and $g = (-1)^{1+n(n-1)/2}$, then $m' = 1 - (-1+i)^{2n-1}$ is divisible by $2 - i$, and hence m is divisible by 5. If $g = (-1)^{n(n-1)/2}$, then $m' = 1 + (-1+i)^{2n-1}$ can be prime only if $2n - 1$ is prime.

The numbers of the form $m = 2^{2n-1} - 2^n + 1$ which are not divisible by 5 belong to the sets mentioned in Example 3 for any $n \not\equiv 1 \pmod 4$, and thus Test 4 can be applied to them. Indeed, if $n \equiv 0 \pmod 4$, then m belongs to the set from Example 3 in case A-III, $g = 1$, and if $n \equiv 2$ or $3 \pmod 4$, then m is divisible by 5. Similarly, the numbers of the form $m = 2^{2n-1} + 2^n + 1$ which are not divisible by 5 belong to the sets mentioned in Example 3 for any n. Indeed, if $n \equiv 0$ or $1 \pmod 4$, then m is divisible by 5. If $n \equiv 2 \pmod 4$, then m belongs to the set from Example 3 in case C-IX, $g = -1$, and if $n \equiv 3 \pmod 4$, then m belongs to the set from Example 3 in case B-V, $g = -1$.

Notice that for $m = g^2 2^{2n} + 1 \in M$ (resp. $m = 2^{2n-1} \pm 2^n + 1 \in M$) we have $m = h2^n + 1$ with $h = g^2$ (resp. $h = 2^{n-1} \pm 1$). Since $h < 2^n$, one can apply the approach of Section 4 to these numbers. In particular, the sets from Example 3 (resp. the sets from Example 3 with $|g| = 1$) can be tested with Test 1 applied to Example 1, where the value of z should correspond either to z or to t from Example 3. The numbers $g^2 2^{2n-1} - g2^n + 1$ with $|g| \neq 1$ cannot be written in the form required in Sections 4 or 5, and thus the corresponding toric test cannot be applied to them.

8. Elliptic tests for $m = g^2 2^{2n} - g2^n + 1$

Fix an odd integer g and suppose that $M \subset \{g^2 2^{2n} - g2^n + 1 \mid n \geqslant 2,\ |g| < 2^n - 2,\ 3 \mid g2^n - 1\}$. Further suppose that $3 \in S$. Let $d \in \mathbb{Z}_S$, $p \nmid d$ for any $p \in \mathbb{P} \setminus S$. We are going to check primality of the elements of M with the aid of the elliptic curve G given by the equation $y^2 = x^3 + d$.

Remark 4. We have $\eta^2(x) = \frac{\eta(x)^4 - 8d\eta(x)}{4(\eta(x)^3 + d)} = \frac{\eta(x)^4 - 8d\eta(x)}{4\eta(y)^2}$ for any $\eta \in G(K)$ different from the identity, where K is a field such that $\operatorname{char} K \notin S$.

Lemma 8. *Let $p \in \mathbb{P} \setminus S$, $\eta \in G(\mathbb{F}_p)$. Then η is of order 2 if and only if $\eta(x^3 + d) = 0$.*

Proof. It follows immediately from Remark 4. □

Denote $\omega = (-1 + \sqrt{3}i)/2$. Let $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 3$, $\zeta \in \mathbb{F}_p$ be such that $\zeta^2 + \zeta + 1 = 0$. Define a map $\omega : G(\mathbb{F}_p) \to G(\mathbb{F}_p)$ as follows: $\omega(x, y) = (\zeta x, y)$. Clearly, ω is an endomorphism of $G(\mathbb{F}_p)$, and thus $G(\mathbb{F}_p)$ gets a structure of $\mathbb{Z}[\omega]$-module.

Lemma 9. *(Cf. [2, Proposition 10].) Let $p \in \mathbb{P} \setminus S$, $p \equiv 1 \pmod 3$, be such that $\#G(\mathbb{F}_p) = h2^{2n}$, $2 \nmid h$. Then $G(\mathbb{F}_p) \cong \mathbb{Z}[\omega]/2^n\mathbb{Z}[\omega] \oplus H$ as $\mathbb{Z}[\omega]$-modules, where H is a $\mathbb{Z}[\omega]$-module, $\#H = h$.*

Proof. Since $G(\mathbb{F}_p)$ is a finitely generated $\mathbb{Z}[\omega]$-module, it must be isomorphic to $\bigoplus_{l=1}^{k} \mathbb{Z}[\omega]/\theta_l\mathbb{Z}[\omega]$, where $\theta_1, \ldots, \theta_k \in \mathbb{Z}[\omega]$ are powers of primes in $\mathbb{Z}[\omega]$, and $\#G(\mathbb{F}_p) = \prod_{l=1}^{k} N(\theta_l)$. Since 2 is the only prime in $\mathbb{Z}[\omega]$ with norm divisible by 2, there exists $0 \leqslant \tilde{k} \leqslant k$ such that θ_l is a power of 2 for any $1 \leqslant l \leqslant \tilde{k}$, and $N(\theta_l)$ is odd for any $\tilde{k} < l \leqslant k$. Put $H = \bigoplus_{l=\tilde{k}+1}^{k} \mathbb{Z}[\omega]/\theta_l\mathbb{Z}[\omega]$. Further, it is clear that $\mathbb{Z}[\omega]/2^j\mathbb{Z}[\omega]$ has 2^{2j} elements three of which are of order 2 for any $j \geqslant 1$. Finally, Remark 4 implies that in $G(\mathbb{F}_p)$ viewed as a $\mathbb{Z}[\omega]$-module, there are at most three elements of order 2. Thus $\tilde{k} \leqslant 1$ and $G(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}[\omega]/2^n\mathbb{Z}[\omega] \oplus H$. □

For $m = g^2 2^{2n} - g2^n + 1 \in M$, define

$$m' = -1 + \bigl(g2^n - 1\bigr)\omega. \tag{3}$$

We have $N(m') = m$ where $N : \mathbb{Q}(\omega) \to \mathbb{Q}$ denotes the norm map. If $p \in \mathbb{P} \cap M$, then p' must be prime in the ring $\mathbb{Z}[\omega]$.

Proposition 9. *If $p = g^2 2^{2n} - g2^n + 1 \in \mathbb{P} \cap M$ and $(\frac{4d}{p'})_6 = -\omega^2$, then $\#G(\mathbb{F}_p) = g^2 2^{2n}$ and $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$ as abelian groups, where H is an abelian group, $\#H = g^2$.*

Proof. We have $g2^n - 1 \equiv 0 \pmod 3$. Therefore, according to [13, Theorem 4 in §18.3], we get

$$\begin{aligned}\#G(\mathbb{F}_p) &= p + 1 - \omega\bigl(-1 + \bigl(g2^n - 1\bigr)\omega\bigr) - \omega^2\bigl(-1 + \bigl(g2^n - 1\bigr)\omega^2\bigr)\\ &= g^2 2^{2n} - g2^n + 1 + 1 + \omega - g2^n\omega^2 + \omega^2 + \omega^2 - g2^n\omega + \omega = g^2 2^{2n}.\end{aligned}$$

Finally, Lemma 9 implies $G(\mathbb{F}_p) \cong \mathbb{Z}[\omega]/2^n\mathbb{Z}[\omega] \oplus H$ as $\mathbb{Z}[\omega]$-modules. Thus $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$ as abelian groups. □

Lemma 10. *Let $m = g^2 2^{2n} - g2^n + 1 \in M$, $p \in \mathbb{P}$, $p \mid m$, $\eta \in G(\mathbb{F}_p)$, $l \in \mathbb{Z}$. If the order of η in $G(\mathbb{F}_p)$ is 2^l, then $\#G(\mathbb{F}_p) \geqslant 2^{2l}$.*

Proof. Since the equation $x^2 - x + 1 \equiv 0 \pmod p$ has a solution $x = g2^n$, we get $p \equiv 1 \pmod 3$. Thus $G(\mathbb{F}_p)$ has a $\mathbb{Z}[\omega]$-module structure. The ideal of $\mathbb{Z}[\omega]$ which annihilates η must be $2^l\mathbb{Z}[\omega]$. Then the $\mathbb{Z}[\omega]$-submodule of $G(\mathbb{F}_p)$ generated by η contains 2^{2l} elements. □

Proposition 10. *Let $z \in S$ be such that $(\frac{z}{p}) = -1$ for any $p \in \mathbb{P} \cap M$. Let $v \in \mathbb{Z}_S$ be such that*

$$\lambda^2 v^4 - 3\lambda v^2 + 3 = z,$$

where $\lambda \in \{1, 2, -1, -2\}$. Then setting $\beta(x) = e(\lambda v^2 - 1)$, $\beta(y) = e^2 v$ defines a point $\beta \in G(\mathbb{Z}_S)$ with $d = e^3$, $e = \lambda z$, and for any $p = g^2 2^{2n} - g2^n + 1 \in \mathbb{P} \cap M$, the order of $r_p(\alpha)$ in $G(\mathbb{F}_p)$ is equal to 2^n, where $\alpha = \beta^{g^2}$.

Proof. We have $\beta(x)^3 + d = e^3(\lambda v^2 - 1)^3 + e^3 = e^3(\lambda^3 v^6 - 3\lambda^2 v^4 + 3\lambda v^2) = e^3\lambda v^2(\lambda^2 v^4 - 3\lambda v^2 + 3) = e^3\lambda v^2 z = \beta(y)^2$ and hence β is a point on G. Further, one can notice that $(\frac{\lambda}{p}) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $(\frac{4d}{p'})_6 \equiv (4e^3)^{\frac{p-1}{6}} = 2^{\frac{p-1}{3}} e^{\frac{p-1}{2}} \equiv (\frac{2}{p'})_3 (\frac{e}{p}) = -(\frac{2}{p'})_3 \pmod{p'}$ (here p' is given by formula (3)). Applying the cubic reciprocity law [13, Theorem 1 in §9.3] we obtain $(\frac{4d}{p'})_6 = -(\frac{2}{p'})_3 = -(\frac{p'}{2})_3 = -(\frac{-1-\omega}{2})_3 = -\omega^2$. Then Proposition 9 implies that $\#G(\mathbb{F}_p) = g^2 2^{2n}$ and $G(\mathbb{F}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus H$, where $\#H = g^2$. Now, we show that $r_p(\beta)$ is not a square in $G(\mathbb{F}_p)$. Let $\eta \in G(\mathbb{F}_p)$ be such that $\eta^2 = r_p(\beta)$. In $G(\mathbb{F}_p)$ there are four distinct elements, say δ_i, $1 \leqslant i \leqslant 4$, such that δ_i^2 is the identity in $G(\mathbb{F}_p)$. Then we have $(\delta_i\eta)^2 = r_p(\beta)$ for any $1 \leqslant i \leqslant 4$. Moreover, $\delta_i\eta(x) \neq \delta_j\eta(x)$ for $i \neq j$, since otherwise $r_p(\beta)^2 = (\delta_i\eta)^2(\delta_j\eta)^2 = (\delta_i\eta\delta_j\eta)^2$ should be the identity in $G(\mathbb{F}_p)$, i.e. $r_p(\beta)$ should be one of δ_i which is impossible. Thus according to Remark 4, the polynomial $\mathcal{P}(x) = x^4 - 4eux^3 - 8e^3x - 4e^4u$, where $u = (\lambda v^2 - 1)$, has four distinct roots in $\mathbb{F}_p$. On the other hand, $\mathbb{F}_p(r)$, where $r^2 = z$, is a quadratic extension of $\mathbb{F}_p$, and in the ring $\mathbb{F}_p(r)[x]$ we have the following decomposition of $\mathcal{P}$:

$$\mathcal{P}(x) = \big(x^2 - 2e(u - r)x - 2e^2(u - 1 - r)\big)\big(x^2 - 2e(u + r)x - 2e^2(u - 1 + r)\big).$$

Hence the product of two of the roots of $\mathcal{P}$ must be equal to $-2e^2(\lambda u^2 - 2 + r)$. This implies that r must belong to $\mathbb{F}_p$ which gives a contradiction. Therefore $r_p(\beta)$ is not a square in $G(\mathbb{F}_p)$. Since g^2 is odd, $r_p(\alpha)$ is not a square in $G(\mathbb{F}_p)$ either. Thus $r_p(\alpha)$ must be of order 2^n. □

Test 5. *Let d, α be as in Proposition 10. Define a sequence $b_i \in \mathbb{Z}_S$ by $b_0 = \alpha(x)$, $b_{i+1} = \frac{b_i^4 - 8db_i}{4(b_i^3 + d)}$. Then $m = g^2 2^{2n} - g2^n + 1 \in M$ is prime if and only if $(m, b_i^3 + d) = 1$ for any $0 \leqslant i \leqslant n - 2$ and $m \mid b_{n-1}^3 + d$.*

Proof. Let $U = \operatorname{Spec}\mathbb{Z}_S[x, y]/(y^2 - x^3 - d)$ be the standard affine chart of G. Take $f = x^3 + d$, $\psi(x) = (\sqrt{x} + 1)^2$, $\rho(x) = x^2$ and $\xi(g^2 2^{2n} - g2^n + 1) = 2^n$. Then Lemma 8 implies that assumption (i) is satisfied. Assumption (ii) follows from Hasse's theorem. Lemma 10 implies that assumption (iii) is satisfied. According to Proposition 10, assumption (iv) is also satisfied. Finally, assumption (v) follows from $g^2 2^{2n} - g2^n + 1 < (2^n - 1)^4$ which holds for any $n \geqslant 2$, since $g^2 < 2^{2n} - 4 \cdot 2^n + 4$ and $|g| < 2 \cdot 2^n - 4$. Thus Theorem 1 implies that m is prime if and only if $r_m(\alpha^{2^{n-1}}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{2^{n-1}})(x^3 + d) = 0$. Now if $m \in \mathbb{P} \cap M$, then $r_m(\alpha^{2^{n-1}}) \in U(\mathbb{Z}/m\mathbb{Z})$ implies $r_m(\alpha^{2^i}) \in U(\mathbb{Z}/m\mathbb{Z})$ for any $1 \leqslant i \leqslant n - 1$. Moreover, according to Remark 4, we get $(m, r_m(\alpha^{2^{i-1}})(x^3 + d)) = 1$ and $r_m(\alpha^{2^i})(x) \equiv b_i \pmod m$ for any $1 \leqslant i \leqslant n - 1$. Hence $(m, b_i^3 + d) = 1$ for any $0 \leqslant i \leqslant n - 2$, and $r_m(\alpha^{2^{n-1}})(x^3 + d) = 0$ implies

$m \mid b_{n-1}^3 + d$. Conversely, if $(m, b_i^3 + d) = 1$ for any $0 \leqslant i \leqslant n-2$ and $m \mid b_{n-1}^3 + d$, then $r_m(\alpha^{2^i}) \in U(\mathbb{Z}/m\mathbb{Z})$ and $r_m(\alpha^{2^i})(x) \equiv b_i \pmod m$ for any $1 \leqslant i \leqslant n-1$. Therefore $r_m(\alpha^{2^{n-1}})(x^3 + d) \equiv b_{n-1}^3 + d \equiv 0 \pmod m$. □

Example 5. Here are some possible choices of parameters satisfying the hypotheses of Proposition 10 and assumption $(*)$ for two values of z.

Case A: $z = 7$, $S = \{2, 3, 7\}$.
1) $\lambda = -1$, $v = 1$, $d = -343$, $\beta(x) = 14$, $\beta(y) = 49$.
2) $\lambda = 1$, $v = 2$, $d = 343$, $\beta(x) = 21$, $\beta(y) = 98$.
I) $g \equiv -5, 13$, or $-17 \pmod{42}$, $M = \{g^2 2^{12l} - g2^{6l} + 1 \mid l \geqslant 1,\ g < 2^{6l} - 2\}$.
II) $g \equiv -13, 17$ or $-19 \pmod{42}$, $M = \{g^2 2^{12l+2} - g2^{6l+1} + 1 \mid l \geqslant 1,\ g < 2^{6l+1} - 2\}$.
III) $g \equiv 1, -17$ or $19 \pmod{42}$, $M = \{g^2 2^{12l+4} - g2^{6l+2} + 1 \mid l \geqslant 0,\ g < 2^{6l+2} - 2\}$.
IV) $g \equiv -1, 11$ or $-19 \pmod{42}$, $M = \{g^2 2^{12l+6} - g2^{6l+3} + 1 \mid l \geqslant 0,\ g < 2^{6l+3} - 2\}$.
V) $g \equiv 1, -5$ or $-11 \pmod{42}$, $M = \{g^2 2^{12l+8} - g2^{6l+4} + 1 \mid l \geqslant 0,\ g < 2^{6l+4} - 2\}$.
VI) $g \equiv 5, 11$ or $-13 \pmod{42}$, $M = \{g^2 2^{12l+10} - g2^{6l+5} + 1 \mid l \geqslant 0,\ g < 2^{6l+5} - 2\}$.
$m \equiv -1$ or $3 \pmod 7$ for any $m \in M$, $(\frac{7}{p}) = (\frac{p}{7}) = -1$ for any $p \in \mathbb{P} \cap M$.

Case B: $z = 13$, $S = \{2, 3, 13\}$, $\lambda = -2$, $v = 1$, $d = -17\,576$, $\beta(x) = 78$, $\beta(y) = 676$.

Since for n not divisible by 3 we have $g^2 2^{2n} - g2^n + 1 = N(g(2\omega)^n + 1)$, the number $2^{2n} - 2^n + 1$ can be prime only if n is either divisible by 3 or equal to a power of 2. The test by Denomme and Savin for the numbers of the form $2^{2^{l+1}} - 2^{2^l} + 1$ [2, Theorem in §9] can be obtained by applying Test 5 to Example 5 in case A-2-III, V, $g = 1$, and replacing the sequence b_i by the sequence $a_i = b_i/7$.

Notice that since $2^{2^{l+1}} - 2^{2^l} + 1 = h2^n + 1$ with $h = 2^{2^l} - 1 < 2^{2^l}$, one can apply the approach of Section 4 to these numbers. They can be tested with Test 1 applied to Example 1 in case C-II, III. The numbers $g^2 2^{2n} - g2^n + 1$ with $g \neq 1$ cannot be written in the form required in Sections 4 and 5, and thus the corresponding toric test cannot be applied to them.

Acknowledgments

Kunyavskiĭ was supported in part by the Minerva foundation through the Emmy Noether Research Institute. This work was finished when he was visiting the MPIM (Bonn) in September 2010. The support of these institutions is gratefully appreciated. We thank the referees for careful reading and thoughtful critical remarks.

References

[1] B.H. Gross, An elliptic curve test for Mersenne primes, J. Number Theory 110 (2005) 114–119.
[2] R. Denomme, G. Savin, Elliptic curve primality test for Fermat and related primes, J. Number Theory 128 (2008) 2398–2412.
[3] H.C. Williams, Édouard Lucas, Primality Testing, CMS Ser. Monogr. Adv. Texts, vol. 22, John Wiley & Sons, New York, 1998.
[4] C. Pomerance, Primality testing: variations on a theme of Lucas, Congr. Numer. 201 (2010) 301–312.
[5] D. Bernstein, Distinguishing prime numbers from composite numbers: the state of the art in 2004, http://cr.yp.to/papers.html#prime2004.
[6] A. Gurevich, B. Kunyavskiĭ, Primality testing through algebraic groups, Arch. Math. 93 (2009) 555–564.
[7] R. Schoof, Nonsingular plane cubic curves over finite fields, J. Combin. Theory Ser. A 46 (1987) 183–211.
[8] D.V. Chudnovsky, G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Adv. Appl. Math. 7 (1986) 385–434.
[9] R. Crandall, C. Pomerance, Prime Numbers. A Computational Perspective, second ed., Springer-Verlag, New York, 2005.
[10] P. Mihăilescu, Algorithms for generating, testing and proving primes: a survey, in: K.-Y. Lam, I. Shparlinski, H. Wang, C. Xing (Eds.), Cryptography and Computational Number Theory, in: Progr. Comput. Sci. Appl. Logic, vol. 20, Birkhäuser, Basel–Boston–Berlin, 2001, pp. 93–122.
[11] M. Kida, Primality tests using algebraic groups, Experiment. Math. 13 (2004) 421–427.
[12] W.C. Waterhouse, B. Weisfeiler, One-dimensional affine group schemes, J. Algebra 66 (1980) 550–568.
[13] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Springer-Verlag, New York, 1990.