Max-Planck-Institut für Mathematik
Bonn

Deterministic primality tests based on tori and elliptic curves

by

Alexander Gurevich
Boris Kunyavskiĭ

Max-Planck-Institut für Mathematik
Preprint Series 2010 (91)

Deterministic primality tests based on tori and elliptic curves

Alexander Gurevich
Boris Kunyavskiĭ

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

The Hebrew University of Jerusalem
Givat Ram
91904 Jerusalem
Israel

Bar-Ilan University
52900 Ramat Gan
Israel

MPIM 10-91

Deterministic primality tests based on tori and elliptic curves

Alexander Gurevich
The Hebrew University of Jerusalem
Givat Ram, 91904 Jerusalem, Israel
gurevich@math.huji.ac.il

Boris Kunyavskiĭ
Bar-Ilan University
52900 Ramat Gan, Israel
kunyav@macs.biu.ac.il

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.

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 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]. In the present note, our purpose is to unify the aforementioned deterministic tests and develop new ones for numbers which were not considered earlier.

We keep following the approach presented in our previous article [3] 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 1) which allows us to shorten the proofs of the toric tests for the numbers of the form $h2^n \pm 1$ (Sections 2 and 3) and include several elliptic tests for the same numbers (Sections 4 and 5). Moreover, we develop elliptic tests for the numbers of the form $g^2 2^{2n-1} - g2^n + 1$ (Section 5) and of the form $g^2 2^{2n} - g2^n + 1$ (Section 6) which, as far as we know, cannot be tested with a toric test.

In Section 4, 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 [4] 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 5, the general test is applied to the same elliptic curve as in Section 4, 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 [5], 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 6, 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.

1 General test

We start with formulating a general deterministic primality test which is a modification of the test introduced in [3].

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 $s \in S$, $m \in M$.

Let G be a group scheme defined over $\mathbb{Z}_S = \{n_1/n_2 \in \mathbb{Q} \mid n_1, n_2 \in \mathbb{Z}, p \nmid n_2$ for any $p \in \mathbb{P} \setminus S\}$. Let m be such that $s \nmid m$ for any $s \in S$. Denote by $r_m \colon G(\mathbb{Z}_S) \to G(\mathbb{Z}/m\mathbb{Z})$ the reduction modulo m.

Suppose that we have an open affine subscheme $U = \operatorname{Spec} A$ of G, a function $f \in A$ on U, an increasing function $\psi \colon \mathbb{R}^+ \to \mathbb{R}^+$, a function $\rho \colon \{2^l \mid l \in \mathbb{Z}\} \to \mathbb{R}^+$, a point $\alpha \in U(\mathbb{Z}_S) = \operatorname{Hom}_{\mathbb{Z}_S}(A, \mathbb{Z}_S)$ (we regard R-valued points on U as $\mathbb{Z}_S$-morphisms from A to R), and a function $\xi \colon M \to \{2^l \mid l \in \mathbb{Z}\}$ 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 in $G(\mathbb{F}_p)$ is equal to 2 if and only if $\eta \in U(\mathbb{F}_p) = \operatorname{Hom}_{\mathbb{Z}_S}(A, \mathbb{F}_p)$ and $\eta(f) = 0$;

(ii) for every $p \in \mathbb{P} \setminus S$, we have $\#G(\mathbb{F}_p) \le \psi(p)$;

(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 $\rho(2^l) \le \#G(\mathbb{F}_p)$;

(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 $\psi(\sqrt{m}) < \rho(\xi(m))$.

Here are some comments on the meaning of these assumptions: (i) allows one to detect elements of order 2, (ii) gives an upper estimate for the order of the group under consideration, (iii) gives a lower estimate for the order of the group through the order of one of its points, (iv) fixes the order of the point in the case where the tested number is prime. 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 $\psi(\sqrt{m}) < \rho(\xi(m)) \le \#G(\mathbb{F}_p) \le \psi(p)$. Since ψ is an increasing function, we get $\sqrt{m} < p$. Thus m must be prime. □

2 Toric tests for $m = h2^n + 1$

Fix an odd positive integer h and suppose that $M \subset \{h2^n + 1 \mid n \ge 1, h < 2^n\}$. 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, η is of order 2 in $G(\mathbb{F}_p)$ if and only if $\eta(x) + 1 = 0$ for any $\eta \in G(\mathbb{F}_p)$. 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 $\left(\frac{\gamma(x)}{p}\right) = -1$, then $r_p(\gamma)$ is not a square in $G(\mathbb{F}_p)$.

Proposition 1. *Let $z \in S$ be such that $\left(\frac{z}{p}\right) = -1$ 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. [3, 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 $i \geq 0$. Further, take $U = G$, $f = x + 1$, $\psi(x) = x - 1$, $\rho(x) = x$ 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) $h \equiv 1 \pmod 6$, $M = \{h2^{2l} + 1 \mid l \geq 1, h < 2^{2l}\}$.
II) $h \equiv -1 \pmod 6$, $M = \{h2^{2l+1} + 1 \mid l \geq 0, h < 2^{2l+1}\}$.
$m \equiv -1 \pmod 3$ for any $m \in M$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$ for any $p \in \mathbb{P} \cap M$.

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

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

Pepin's test for Fermat numbers [6, Theorem 4.1.2] is none other than Test 1 applied to Example 1 in case A-I, $h = 1$.

3 Toric tests for $m = h2^n - 1$

Fix an odd positive integer h and suppose that $M \subset \{h2^n - 1 \mid n \geq 3, h < 2^n - 2\}$. 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 [7, 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 $x \mapsto x \otimes 1 + 1 \otimes x + 2y \otimes y + 2dx \otimes x$, $y \mapsto y \otimes 1 + 1 \otimes y + 2dy \otimes x + 2dx \otimes y$.

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 in $G(\mathbb{F}_p)$ 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 $\#G(\mathbb{F}_p) = p - \left(\frac{d}{p}\right)$, and the group $G(\mathbb{F}_p)$ is cyclic.*

Proof. This immediately follows from [7, 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 $\left(\frac{\gamma(x)}{p}\right) = -1$, 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 $\left(\frac{z}{p}\right) = -1$ 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 $\kappa \in \{1, -z\}$, $\lambda, \mu \in \{1, 2\}$. 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 $\beta(y)^2 - d\beta(x)^2 = (\kappa^2u^2v^2 - \lambda z\kappa v^4)/\mu^2 = -\kappa\mu v^2/\mu^2 = \beta(x)$, and hence β is a point on G. Furthermore, one can notice that $\left(\frac{\kappa}{p}\right) = \left(\frac{\lambda}{p}\right) = \left(\frac{\mu}{p}\right) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $\left(\frac{d}{p}\right) = \left(\frac{\beta(x)}{p}\right) = -1$. 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. [3, 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 $i \geq 0$ 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) $h \equiv -1 \pmod 6$, $M = \{h2^{2l} - 1 \mid l \geq 2, h < 2^{2l} - 2\}$.
II) $h \equiv 1 \pmod 6$, $M = \{h2^{2l+1} - 1 \mid l \geq 1, h < 2^{2l+1} - 2\}$.
$m \equiv 1 \pmod 3$ *for any* $m \in M$, $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1$ *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* $3 \pmod{10}$, $M = \{h2^{4l} - 1 \mid l \geq 1, h < 2^{4l} - 2\}$.
II) $h \equiv -1$ *or* $-3 \pmod{10}$, $M = \{h2^{4l+1} - 1 \mid l \geq 1, h < 2^{4l+1} - 2\}$.
III) $h \equiv 1$ *or* $-3 \pmod{10}$, $M = \{h2^{4l+2} - 1 \mid l \geq 1, h < 2^{4l+2} - 2\}$.
IV) $h \equiv 1$ *or* $3 \pmod{10}$, $M = \{h2^{4l+3} - 1 \mid l \geq 1, h < 2^{4l+3} - 2\}$.
$m \equiv 2$ *or* $-2 \pmod 5$ *for any* $m \in M$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$ *for any* $p \in \mathbb{P} \cap M$.

The classical Lucas–Lehmer test for Mersenne numbers [6, 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 [3, Corollary 3.8]).

4 Elliptic tests for $m = h2^n - 1$

Fix an odd positive integer h and suppose that $M \subset \{h2^n - 1 \mid n \geq 3, h < 2^n - 2^{(n+4)/2}\}$. 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 *in* $G(\mathbb{F}_p)$ *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* $\left(\frac{d}{p}\right) = 1$.

Proof. According to [8, Theorem 5 in §18.4], we have $\#G(\mathbb{F}_p) = p+1$. Further, [4, 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 $\left(\frac{d}{p}\right) = -1$, 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 $\left(\frac{\gamma(x)}{p}\right) = -1$, 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 $\left(\frac{z}{p}\right) = -1$ 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 $\left(\frac{\kappa}{p}\right) = \left(\frac{\lambda}{p}\right) = \left(\frac{\mu}{p}\right) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $\left(\frac{d}{p}\right) = \left(\frac{\beta(x)}{p}\right) = -1$. 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 $0 \le i \le n-2$ 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 $1 \le i \le n-1$. 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 $1 \le i \le n-1$. Hence $(m, b_i^3 - db_i) = 1$ for any $0 \le i \le n-2$, 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 $0 \le i \le n-2$ 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 $1 \le i \le n-1$. 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, $h = 1$.

5 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 $M \subset \{g^2 2^{2n} + 1 \mid n \geq 3, |g| < 2^{n-1} - 2\}$ (resp. $M \subset \{g^2 2^{2n-1} - g2^n + 1 \mid n \geq 3, |g| < 2^{n-1/2} - 2\}$). 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 $i\colon G(\mathbb{F}_p) \to G(\mathbb{F}_p)$ 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 $\oplus_{l=1}^k \mathbb{Z}[i]/\theta_l\mathbb{Z}[i]$, 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 $0 \leq \tilde{k} \leq k$ such that θ_l is a power of $1+i$ for any $1 \leq l \leq \tilde{k}$, and $N(\theta_l)$ is odd for any $\tilde{k} < l \leq k$. Put $H = \oplus_{l=\tilde{k}+1}^k \mathbb{Z}[i]/\theta_l\mathbb{Z}[i]$. 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 $N\colon \mathbb{Q}(i) \to \mathbb{Q}$ 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 $\left(\frac{d}{p'}\right)_4 = 1$, 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 [8, Theorem 5 in §18.4], we get

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

Thus $\#G(\mathbb{F}_p) = g^2 2^{2n}$ (resp. $\#G(\mathbb{F}_p) = g^2 2^{2n-1}$). Finally, Lemma 5 implies $G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n}\mathbb{Z}[i] \oplus H$ (resp. $G(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2n-1}\mathbb{Z}[i] \oplus H$) 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 $\#G(\mathbb{F}_p) \geq 2^{2l-1}$.*

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

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

where $\kappa, \lambda, \mu \in \{1, 2, -1, -2\}$. Then setting $\beta(x) = e\lambda z v^2$, $\beta(y) = e^2 uvw$ defines a point $\beta \in G(\mathbb{Z}_S)$ with $d = e^2$, $e = \kappa\lambda\mu z t$, 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 $\left(\frac{\kappa}{p}\right) = \left(\frac{\lambda}{p}\right) = \left(\frac{\mu}{p}\right) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $\left(\frac{d}{p'}\right)_4 \equiv d^{\frac{p-1}{4}} = e^{\frac{p-1}{2}} \equiv \left(\frac{e}{p}\right) = 1 \pmod{p'}$, $\left(\frac{\beta(x)}{p}\right) = -1$, 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 $\left(\frac{z}{p}\right) = -1$, $\left(\frac{zt}{p'}\right)_4 = 1$ 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 $\beta(x) = \kappa\lambda^2 z v^2$, $\beta(y) = \kappa^2\lambda^2 zuv$ 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 $\left(\frac{\kappa}{p}\right) = \left(\frac{\lambda}{p}\right) = \left(\frac{\mu}{p}\right) = 1$ for any $p \in \mathbb{P} \cap M$, and hence, $\left(\frac{d}{p'}\right)_4 = \left(\frac{\kappa^2\lambda^2\mu^2}{p'}\right)_4 \equiv (\kappa^2\lambda^2\mu^2)^{\frac{p-1}{4}} = (\kappa\lambda\mu)^{\frac{p-1}{2}} \equiv \left(\frac{\kappa\lambda\mu}{p}\right) = 1 \pmod{p'}$, $\left(\frac{\beta(x)}{p}\right) = -1$. 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 $0 \le i \le n-2$ 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 $n \ge 3$, since $g^2 < 2^{2n-2} - 4 \cdot 2^{n-1} + 4 < 2^{2n-2} - 4 \cdot 2^{(2n-3)/2}$ (resp. $g^2 < 2^{2n-1} - 4 \cdot 2^{(2n-1)/2} + 4$ and $|g| < 2^n - 2^{3/2}$). 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 $r_m(\alpha^{2^{n-1}})(x^3 - dx) = 0$. 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: $z = 5$, $t = 3$, $S = \{2, 3, 5\}$,
$\kappa = 1$, $\lambda = 1$, $\mu = 2$, $u = 2$, $v = 1$, $w = 1$.
I) $g \equiv \pm 1$ *or* $\pm 11 \pmod{30}$, $M = \{g^2 2^{4l} + 1 \mid l \geq 2, g < 2^{2l-1} - 2\}$.
II) $g \equiv \pm 7$ *or* $\pm 13 \pmod{30}$, $M = \{g^2 2^{4l+2} + 1 \mid l \geq 1, g < 2^{2l} - 2\}$.
III) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l-1} - g 2^{4l} + 1 \mid l \geq 1, g < 2^{4l-1/2}\}$.
IV) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+1} - g 2^{4l+1} + 1 \mid l \geq 1, g < 2^{4l+1/2}\}$.
V) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+3} - g 2^{4l+2} + 1 \mid l \geq 1, g < 2^{4l+3/2}\}$.
VI) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+5} - g 2^{4l+3} + 1 \mid l \geq 0, g < 2^{4l+5/2}\}$.
$m \equiv 2$ *or* $-2 \pmod 5$, $m \equiv -1 \pmod 3$ *for any* $m \in M$,
$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$ *for any* $p \in \mathbb{P} \cap M$.

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

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

$M = \{g^2 2^{8l+3} - g2^{4l+2} + 1 \mid l \geq 1, g < 2^{4l+3/2} - 2\}$.

X) $g \equiv 17, -23$ *or* $27 \pmod{70}$,

$M = \{g^2 2^{8l+5} - g2^{4l+3} + 1 \mid l \geq 1, g < 2^{4l+5/2} - 2\}$.

$m \equiv 2$ *or* $-2 \pmod 5$, $m \equiv -1, -2$ *or* $3 \pmod 7$ *for any* $m \in M$,

$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$, $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1$ *for any* $p \in \mathbb{P} \cap M$.

For any $p \in \mathbb{P} \cap M$ we have $\left(\frac{-1}{p'}\right)_4 \equiv (-1)^{\frac{p-1}{4}} = 1 \pmod{p'}$. 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 [8, Theorem 2 in §9.9] implies $\left(\frac{q}{p'}\right)_4 = \left(\frac{(-1)^{(q-1)/2} q}{p'}\right)_4 = \left(\frac{p'}{q}\right)_4$.

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: $z = 5$, $t = 3$, $S = \{2, 3, 5\}$,

$\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 1$, $v = 1$.

I) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l} + 1 \mid l \geq 1, g < 2^{4l-1} - 2\}$.

II) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+2} + 1 \mid l \geq 1, g < 2^{4l} - 2\}$.

III) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+4} + 1 \mid l \geq 1, g < 2^{4l+1} - 2\}$.

IV) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+6} + 1 \mid l \geq 0, g < 2^{4l+2} - 2\}$.

$m \equiv 2 \pmod 5$, $m' \equiv -1 \pmod{2+i}$, $m' \equiv -i \pmod{2-i}$,

$m' \equiv 1 + i \pmod 3$ *for any* $m \in M$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$,

$\left(\frac{15}{p'}\right)_4 = \left(\frac{p'}{(2+i)\cdot(2-i)\cdot 3}\right)_4 = (-1) \cdot (-i) \cdot (-i) = 1$ *for any* $p \in \mathbb{P} \cap M$.

V) $g \equiv -1 \pmod{30}$, $M = \{g^2 2^{8l} + 1 \mid l \geq 1, g < 2^{4l-1} - 2\}$.

VI) $g \equiv 7 \pmod{30}$, $M = \{g^2 2^{8l+2} + 1 \mid l \geq 1, g < 2^{4l} - 2\}$.

VII) $g \equiv 11 \pmod{30}$, $M = \{g^2 2^{8l+4} + 1 \mid l \geq 1, g < 2^{4l+1} - 2\}$.

VIII) $g \equiv 13 \pmod{30}$, $M = \{g^2 2^{8l+6} + 1 \mid l \geq 0, g < 2^{4l+2} - 2\}$.

$m \equiv 2 \pmod 5$, $m' \equiv i \pmod{2+i}$, $m' \equiv -1 \pmod{2-i}$,

$m' \equiv 1 - i \pmod 3$ *for any* $m \in M$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$,

$\left(\frac{15}{p'}\right)_4 = \left(\frac{p'}{(2+i)\cdot(2-i)\cdot 3}\right)_4 = i \cdot (-1) \cdot i = 1$ *for any* $p \in \mathbb{P} \cap M$.

IX) $g \equiv 1 \pmod{30}$, $M = \{g^2 2^{8l-1} - g2^{4l} + 1 \mid l \geq 1, g < 2^{4l-1/2}\}$.

X) $g \equiv -11 \pmod{30}$, $M = \{g^2 2^{8l+3} - g2^{4l+2} + 1 \mid l \geq 1, g < 2^{4l+3/2}\}$.

$m \equiv -2 \pmod 5$, $m' \equiv -1 \pmod{2+i}$, $m' \equiv i \pmod{2-i}$,

$m' \equiv -1 + i \pmod 3$ *for any* $m \in M$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$,

$\left(\frac{15}{p'}\right)_4 = \left(\frac{p'}{(2+i)\cdot(2-i)\cdot 3}\right)_4 = (-1) \cdot i \cdot i = 1$ *for any* $p \in \mathbb{P} \cap M$.

XI) $g \equiv -7 \pmod{30}$, $M = \{g^2 2^{8l+1} - g2^{4l+1} + 1 \mid l \geq 1, g < 2^{4l+1/2}\}$.

XII) $g \equiv -13 \pmod{30}$, $M = \{g^2 2^{8l+5} - g2^{4l+3} + 1 \mid l \geq 0, g < 2^{4l+5/2}\}$.

$m \equiv -2 \pmod 5$, $m' \equiv -i \pmod{2+i}$, $m' \equiv -1 \pmod{2-i}$,

$m' \equiv -1 - i \pmod 3$ *for any* $m \in M$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$,

$\left(\frac{15}{p'}\right)_4 = \left(\frac{p'}{(2+i)\cdot(2-i)\cdot 3}\right)_4 = (-i) \cdot (-1) \cdot (-i) = 1$ *for any* $p \in \mathbb{P} \cap M$.

Case B: $z = 7$, $t = 3$, $S = \{2, 3, 7\}$

$\kappa = 1$, $\lambda = 1$, $\mu = 1$, $u = 2$, $v = 1$.

Case C: $z = 7$, $t = 5$, $S = \{2, 5, 7\}$,

$\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 1$, $v = 1$.

Case D: $z = 3$, $t = 13$, $S = \{2, 3, 7\}$
$\kappa = -1$, $\lambda = 2$, $\mu = 1$, $u = 1$, $v = 1$.
Case E: $z = 13$, $t = 5$, $S = \{2, 5, 13\}$,
$\kappa = 2$, $\lambda = 1$, $\mu = 1$, $u = 2$, $v = 1$.

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 2 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 2 or 3, and thus the corresponding toric test cannot be applied to them.

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

Fix an odd integer g and suppose that $M \subset \{g^2 2^{2n} - g2^n + 1 \mid n \geq 2, |g| < 2^n - 2, 3 \mid g2^n - 1\}$. 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 *in* $G(\mathbb{F}_p)$ *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 $\omega\colon G(\mathbb{F}_p) \to G(\mathbb{F}_p)$ 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 $\oplus_{l=1}^{k}\mathbb{Z}[\omega]/\theta_l\mathbb{Z}[\omega]$, where $\theta_1, \dots, \theta_k \in \mathbb{Z}[\omega]$ 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 $0 \le \tilde{k} \le k$ such that θ_l is a power of 2 for any $1 \le l \le \tilde{k}$, and $N(\theta_l)$ is odd for any $\tilde{k} < l \le k$. Put $H = \oplus_{l=\tilde{k}+1}^{k}\mathbb{Z}[\omega]/\theta_l\mathbb{Z}[\omega]$. 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 $j \ge 1$. 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 $\tilde{k} \le 1$ 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

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

We have $N(m') = m$ where $N\colon \mathbb{Q}(\omega) \to \mathbb{Q}$ 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 $\left(\frac{4d}{p'}\right)_6 = -\omega^2$, 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 [8, Theorem 4 in §18.3], we get

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

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 $\#G(\mathbb{F}_p) \ge 2^{2l}$.*

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 $\left(\frac{z}{p}\right) = -1$ 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 $\left(\frac{\lambda}{p}\right) = 1$ for any $p \in \mathbb{P} \cap M$, and hence $\left(\frac{4d}{p'}\right)_6 \equiv (4e^3)^{\frac{p-1}{6}} = 2^{\frac{p-1}{3}} e^{\frac{p-1}{2}} \equiv \left(\frac{2}{p'}\right)_3 \left(\frac{e}{p}\right) = -\left(\frac{2}{p'}\right)_3 \pmod{p'}$ (here p' is given by formula (3)). Applying the cubic reciprocity law [8, Theorem 1 in §9.3] we obtain $\left(\frac{4d}{p'}\right)_6 = -\left(\frac{2}{p'}\right)_3 = -\left(\frac{p'}{2}\right)_3 = -\left(\frac{-1-\omega}{2}\right)_3 = -\omega^2$. 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, $1 \le i \le 4$, 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 $1 \le i \le 4$. Moreover, $\delta_i \eta(x) \ne \delta_j \eta(x)$ for $i \ne j$, 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 $\mathcal{P}(x) = x^4 - 4eux^3 - 8e^3 x - 4e^4 u$, 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 $\mathcal{P}$:

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

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 $0 \le i \le n - 2$ 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 $n \ge 2$, 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 $1 \le i \le n-1$. 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 $1 \le i \le n - 1$. Hence $(m, b_i^3 + d) = 1$ for any $0 \le i \le n - 2$, 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 $0 \le i \le n - 2$ 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 $1 \leq i \leq n-1$. 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) $\lambda = -1$, $v = 1$.
2) $\lambda = 1$, $v = 2$.
I) $g \equiv -5, 13,$ *or* $-17 \pmod{42}$,
$M = \{g^2 2^{12l} - g2^{6l} + 1 \mid l \geq 1, g < 2^{6l} - 2\}$.
II) $g \equiv -13, 17$ *or* $-19 \pmod{42}$,
$M = \{g^2 2^{12l+2} - g2^{6l+1} + 1 \mid l \geq 1, g < 2^{6l+1} - 2\}$.
III) $g \equiv 1, -17$ *or* $19 \pmod{42}$,
$M = \{g^2 2^{12l+4} - g2^{6l+2} + 1 \mid l \geq 0, g < 2^{6l+2} - 2\}$.
IV) $g \equiv -1, 11$ *or* $-19 \pmod{42}$,
$M = \{g^2 2^{12l+6} - g2^{6l+3} + 1 \mid l \geq 0, g < 2^{6l+3} - 2\}$.
V) $g \equiv 1, -5$ *or* $-11 \pmod{42}$,
$M = \{g^2 2^{12l+8} - g2^{6l+4} + 1 \mid l \geq 0, g < 2^{6l+4} - 2\}$.
VI) $g \equiv 5, 11$ *or* $-13 \pmod{42}$,
$M = \{g^2 2^{12l+10} - g2^{6l+5} + 1 \mid l \geq 0, g < 2^{6l+5} - 2\}$.
$m \equiv -1$ *or* $3 \pmod{7}$ *for any* $m \in M$, $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1$ *for any* $p \in \mathbb{P} \cap M$.
Case B: $z = 13$, $S = \{2, 3, 13\}$,
$\lambda = -2$, $v = 1$.

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 2 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 2 or 3, and thus the corresponding toric test cannot be applied to them.

Acknowledgements. 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.

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] A. Gurevich, B. Kunyavskiĭ, Primality testing through algebraic groups, Arch. Math. 93 (2009) 555–564.

[4] R. Schoof, Nonsingular plane cubic curves over finite fields, J. Combin. Theory, Ser. A 46 (1987) 183–211.

[5] 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.

[6] R. Crandall, C. Pomerance, Prime Numbers. A Computational Perspective, second ed., Springer-Verlag, New York, 2005.

[7] W. C. Waterhouse, B. Weisfeiler, One-dimensional affine group schemes, J. Algebra 66 (1980) 550–568.

[8] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Springer-Verlag, New York, 1990.