Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 2398–2412
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Elliptic curve primality tests for Fermat and related primes

Robert Denomme [a], Gordan Savin [b,*]

[a] *Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA*
[b] *Department of Mathematics, University of Utah, Salt Lake City, UT 84112, USA*

Received 5 August 2007; revised 27 November 2007

Available online 21 March 2008

Communicated by David Goss

Abstract

We use elliptic curves with complex multiplication to develop primality tests for Fermat primes and for primes of the form $3^{2^\ell} - 3^{2^{\ell-1}} + 1$ and $2^{2^\ell} - 2^{2^{\ell-1}} + 1$.

1. Introduction

Fermat numbers are integers of the form $F_\ell = 2^{2^\ell} + 1$. Prime numbers of this form are called Fermat primes. Although it is not known if there are infinitely many Fermat primes, primality of a given Fermat number can be verified by Pepin's test. It is an efficient and elegant test, based on the following coincidence: If F_ℓ is prime then the multiplicative group of the finite field $\mathbb{F}_{F_\ell}$ is a cyclic group of order 2^{2^ℓ}, a pure power of 2, and this group is always generated by 3.

The first goal of this paper is to develop a test for Fermat primes using the elliptic curve $y^2 = x^3 - x$. The test is based on the following: If F_ℓ is a prime then the group $E(F_\ell)$ of points modulo F_ℓ on the elliptic curve has (again) order 2^{2^ℓ}. This group is not cyclic. However, something just as interesting holds in this case. More precisely, if $p \equiv 1 \pmod 4$ is a prime

* Corresponding author.
E-mail addresses: denomme.2@osu.edu (R. Denomme), savin@math.utah.edu (G. Savin).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.12.009

(a Fermat prime, for example) then $E(p)$ admits a complex multiplication by $\mathbb{Z}[i]$, the ring of Gaussian integers. We show that

$$E(F_\ell) \cong \mathbb{Z}[i]/(1+i)^{2^\ell}$$

as $\mathbb{Z}[i]$-modules. Let E_n be the quadratic twist $ny^2 = x^3 - x$ of our curve E. If n is a square modulo F_ℓ then $E_n(F_\ell)$ is isomorphic to $E(F_\ell)$. One can now pick n and a rational point P of infinite order on E_n generating $E_n(F_\ell)$, as a $\mathbb{Z}[i]$-module. For example, we can take $P = (5, 2)$ on the curve E_{30}. This data can be then used to formulate and prove a test for Fermat numbers similar to Pepin's test.

A version of the test can be perhaps best described in terms of Gaussian integers. Note that F_ℓ factors $F_\ell = f_\ell \cdot \bar{f}_\ell$ where $f_\ell = 2^{2^{\ell-1}} + i$. Starting with $x_1 = 5$ (the x-coordinate of the point P) define a sequence of Gaussian integers x_m modulo f_ℓ by a recursion formula (complex multiplication by $1+i$)

$$x_{m+1} = \frac{1}{2}\left(\frac{x_m}{i} + \frac{i}{x_m}\right).$$

Then F_ℓ is prime if and only if x_m is relatively prime to f_ℓ for all $m = 1, \ldots, 2^\ell - 1$ and

$$x_{2^\ell} \equiv 0 \pmod{f_\ell}.$$

It is interesting to note that this recursion does not depend on the choice of n. Moreover, there are other choices for the initial value x_1 for which the test works. A similar phenomenon occurs for the Lucas–Lehmer test for Mersenne numbers.

We then move to two other families of integers. We use elliptic curves of the form $y^2 = x^3 + \frac{D}{4}$ to develop two tests, for integers of the form

$$3^{2^\ell} - 3^{2^{\ell-1}} + 1 \quad \text{and} \quad 2^{2^\ell} - 2^{2^{\ell-1}} + 1,$$

respectively. Again, the main role is played by complex multiplication by $\mathbb{Z}[\omega]$, the ring of Eisenstein integers.

2. Pepin's test

In this section we quickly review Pepin's test for Fermat primes. The proof is presented in a way that generalizes to elliptic curves.

Proposition 1. *A Fermat number $F_\ell = 2^{2^\ell} + 1$ is prime if and only if*

$$3^{\frac{F_\ell - 1}{2}} \equiv -1 \pmod{F_\ell}.$$

Proof. Assume first that the congruence holds. Let p be a prime dividing F_ℓ. Then

$$3^{\frac{F_\ell - 1}{2}} \equiv -1 \pmod{p}$$

and, after squaring both sides of the congruence,

$$3^{F_\ell - 1} \equiv 1 \pmod{p}.$$

In particular, the order of 3 modulo p divides $F_\ell - 1$. Since $F_\ell - 1 = 2^{2^\ell}$, a pure power of 2, any proper divisor of $F_\ell - 1$ is a divisor of $\frac{F_\ell - 1}{2}$. Since $3^{\frac{F_\ell - 1}{2}} \not\equiv 1 \pmod{p}$, the order of 3 modulo p is exactly $F_\ell - 1$. On the other hand, the order of 3 modulo p is less than or equal to $p - 1$. This implies

$$F_\ell - 1 \leqslant p - 1$$

or $F_\ell \leqslant p$. It follows that F_ℓ is prime.

The converse is more interesting, for it shows why the test really works. Assume that F_ℓ is prime. Note that $F_\ell \equiv 2 \pmod{3}$. By quadratic reciprocity, 3 is not a square modulo F_ℓ:

$$\left(\frac{3}{F_\ell}\right) = \left(\frac{F_\ell}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Note that the group $\mathbb{F}_{F_\ell}^\times$ has order equal to a pure power of 2 and is cyclic. Since 3 is not a square mod F_ℓ, it must be a generator of $\mathbb{F}_{F_\ell}^\times$. It follows that

$$3^{\frac{F_\ell - 1}{2}}$$

is an element of order 2 in $\mathbb{F}_{F_\ell}^\times$. But -1 is the only element of order 2, and this completes the converse. The test is proved. □

Of course, the number 3 can be replaced by any other number, provided it is not a square modulo F_ℓ. For example, if $F_\ell > 5$ then we can replace 3 by 5. Indeed, if $F_\ell > 5$ then $F_\ell \equiv 2 \pmod{5}$ and, by quadratic reciprocity,

$$\left(\frac{5}{F_\ell}\right) = -1.$$

3. The curve $y^2 = x^3 - x$

We denote the group of the elliptic curve $y^2 = x^3 - x$ over the finite field $\mathbb{F}_p$ by $E(p)$. The discriminant of E is 2^6. In particular E has a good reduction modulo any odd prime p.

Proposition 2. *Let p be an odd prime. If $p \equiv 1 \pmod{4}$ then $|E(p)| = p + 1 - 2a$ where $p = a^2 + b^2$ and $a + bi \equiv 1 \pmod{2 + 2i}$.*

Proof. See [I&R, p. 307]. □

Corollary 3. *For $\ell > 1$ if $F_\ell = 2^{2^\ell} + 1$ is prime, then the group $E(F_\ell)$ satisfies $|E(F_\ell)| = 2^{2^\ell}$.*

Proof. Notice that $F_\ell = 1^2 + (2^{2^{\ell-1}})^2$ and that $\ell > 1 \Rightarrow 4 \mid 2^{2^{\ell-1}}$, which yields the congruence

$$1 + 2^{2^{\ell-1}} i \equiv 1 \pmod{2+2i}.$$

Thus by Proposition 2, $|E(F_\ell)| = F_\ell + 1 - 2 \cdot 1 = 2^{2^\ell}$. □

In order to better understand the structure of the group $E(F_\ell)$, we now introduce a complex multiplication on our curve. If $p \equiv 1 \pmod 4$ let $\pm i$ denote the primitive fourth roots of unity in the finite field $\mathbb{F}_p$. The action

$$i : (x, y) \to (-x, iy)$$

is an endomorphism and thus turns $E(p)$ into a $\mathbb{Z}[i]$-module. Critical to us is the action of $1 + i$ on our curve. This is a degree 2 endomorphism of the elliptic curve. The only non-trivial point annihilated by $1 + i$ is

$$Q = (0, 0).$$

Proposition 4. *Assume that $\ell > 1$ and F_ℓ is prime. Then*

$$E(F_\ell) \cong \mathbb{Z}[i]/(1+i)^{2^\ell}$$

as $\mathbb{Z}[i]$-modules.

Proof. First $E(F_\ell)$ is a finitely generated $\mathbb{Z}[i]$-module and so is isomorphic to the additive group:

$$\mathbb{Z}[i]/(\alpha_1) \oplus \mathbb{Z}[i]/(\alpha_2) \oplus \cdots \oplus \mathbb{Z}[i]/(\alpha_k)$$

for some $k \in \mathbb{N}$ and $\{\alpha_j\} \subseteq \mathbb{Z}[i]$. Now each $\mathbb{Z}[i]/(\alpha_j)$ is a subgroup of $E(F_\ell)$ hence $|\mathbb{Z}[i]/(\alpha_j)| = N(\alpha_j)$ divides the order of $E(F_\ell)$. By Corollary 3, $|E(F_\ell)| = 2^{2^\ell}$ so that $N(\alpha_j) = \alpha_j \overline{\alpha_j}$ must be a power of $2 = -i(1+i)^2$. By uniqueness of factorization, for every j there exists in integer m_j such that

$$(\alpha_j) = \big((1+i)^{m_j}\big).$$

Finally, since multiplication by $1 + i$ is a degree 2 map, the annihilator of $1 + i$ in $E(F_\ell)$ has two elements. This implies that $k = 1$. The proposition is proved. □

We now know that the $E(F_\ell)$ is a cyclic $\mathbb{Z}[i]$-module. In order to build the test we need a point P that generates this module. This is accomplished as follows. Let E_n be the quadratic twist $ny^2 = x^3 - x$ of our elliptic curve E. Here n can be picked to be an integer or a rational number. If n is a non-zero square modulo F_ℓ then

$$(x, y) \mapsto \big(x, n^{\frac{1}{2}} \cdot y\big)$$

is an isomorphism of $\mathbb{Z}[i]$-modules $E_n(F_\ell)$ and $E(F_\ell)$. Rational points on the curve E_n (for some n) are easy to construct. One picks a value for x and factors a square out of $x^3 - x$. For example, if $x = 5$, then $5^3 - 5 = 120 = 30 \cdot 2^2$. This shows that $P = (5, 2)$ is a rational point on the curve E_{30}. Moreover,

$$\left(\frac{30}{F_\ell}\right) = \left(\frac{2}{F_\ell}\right) \cdot \left(\frac{3}{F_\ell}\right) \cdot \left(\frac{5}{F_\ell}\right) = 1 \cdot (-1) \cdot (-1) = 1$$

and 30 is a square modulo F_ℓ.

We need explicit formulae for the multiplication by $1 + i$ on the curve $ny^2 = x^3 - x$. The slope of the line through (x, y) and $(-x, iy)$ is

$$A = \frac{(1-i)y}{2x}.$$

One now easily checks that $(1 + i) \cdot (x, y) = (x', y')$ where

$$\begin{cases} x' = nA^2 = \dfrac{1}{2}\left(\dfrac{x}{i} + \dfrac{i}{x}\right), \\ y' = -y - A(x' - x). \end{cases} \tag{1}$$

Proposition 5. *Let $\ell > 1$ be such that F_ℓ is prime. Then the rational point $P = (5, 2)$ is a generator of the $\mathbb{Z}[i]$-module*

$$E_{30}(F_\ell) \cong \mathbb{Z}[i]/(1+i)^{2^\ell}.$$

Proof. We must show that there is no point R in $E_{30}(F_\ell)$ such that

$$(5, 2) \equiv (1 + i) \cdot R \pmod{F_\ell}.$$

If there is such a point R, then the formula (1) for the action of $1 + i$ on the curve $30y^2 = x^3 - x$ implies that

$$5 \equiv 30 \cdot A^2 \pmod{F_\ell}.$$

Since 30 is a square modulo F_ℓ and 5 is not, this is a contradiction. The proposition is proved. □

Of course, there are other choices for n and P. We can pick $x = 7$. Since $7^3 - 7 = 21 \cdot 4^2$, we have a rational point $P = (7, 4)$ on the curve E_{21}: $21y^2 = x^3 - x$. Using the quadratic reciprocity one easily shows that 7 is not a square modulo Fermat primes and $21 = 3 \cdot 7$ is a square modulo Fermat primes. It follows that the previous proposition holds with the rational point $P = (7, 4)$ on the curve E_{21}.

4. Elliptic curve test for Fermat primes

In this section we develop a test for Fermat primes using the curve $30y^2 = x^3 - x$ and the point $P = (5, 2)$. It is natural to state the test is in terms of Gaussian integers. Note that we have a factorization in $\mathbb{Z}[i]$.

$$F_\ell = f_\ell \cdot \bar{f}_\ell$$

where $f_\ell = 2^{2^{\ell-1}} + i$. Now, F_ℓ is a prime integer if and only if f_ℓ is a Gaussian prime. Recall that $Q = (0, 0)$ is the unique point on the curve $30y^2 = x^3 - x$ of order $1 + i$.

Theorem. *Let $P = (5, 2)$ be a point on the curve E_{30}: $30y^2 = x^3 - x$. Let $\ell > 1$. Then the Fermat number $F_\ell = 2^{2^\ell} + 1$ is prime if and only if*

$$(1+i)^{2^\ell - 1} \cdot P \equiv Q \pmod{f_\ell}$$

where $f_\ell = 2^{2^{\ell-1}} + i$.

Proof. Assume that the congruence holds. We need to show that F_ℓ is prime. If not, then there exists a prime factor p of F_ℓ such that $p < \sqrt{F_\ell}$. The prime p is clearly not equal to 3 or 5. In particular the curve has a good reduction modulo p.

Since p divides F_ℓ,

$$\left(2^{2^{\ell-1}}\right)^2 \equiv -1 \pmod{p}$$

which shows that -1 is a square mod p. In particular, p is not a Gaussian prime and we can write $p = \pi\overline{\pi}$. Without loss of generality, assume that π divides f_ℓ. By assumption, we also have the congruence

$$(1+i)^{2^\ell - 1} \cdot P \equiv Q \pmod{\pi}.$$

Multiplying both sides of this congruence by $1 + i$ gives

$$(1+i)^{2^\ell} \cdot P \equiv O \pmod{\pi}$$

where O is the identity element in $E(\pi)$. It follows that P generates a $\mathbb{Z}[i]$-submodule of $E_{30}(\pi)$ isomorphic to $\mathbb{Z}[i]/((1+i)^{2^\ell})$. The order of this module is $N((1+i)^{2^\ell}) = 2^{2^\ell} = F_\ell - 1$ which implies $F_\ell - 1 \leqslant |E_{30}(\pi)|$. However, by Hasse's estimate, the order of $E(\pi)$ is bounded by

$$\left|E_{30}(\pi)\right| \leqslant p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2.$$

Keeping in mind $p^2 < F_\ell$ we have created the scenario $p^2 - 1 < (\sqrt{p} + 1)^2$ which does not hold for any prime $p > 2$. F_ℓ is odd thus F_ℓ must have been prime to begin with.

For the reverse direction, assume F_ℓ is a prime. Notice that $E_{30}(F_\ell)$ is isomorphic to $E_{30}(f_\ell)$ via the natural isomorphism of the finite fields $\mathbb{Z}/(F_\ell)$ and $\mathbb{Z}[i]/(f_\ell)$. By Proposition 4,

$$E_{30}(f_\ell) \cong \mathbb{Z}[i]/\left((1+i)^{2^\ell}\right),$$

and by Proposition 5, the point P generates this $\mathbb{Z}[i]$-module. It follows that $(1+i)^{2^\ell - 1} \cdot P$ is an element of order $1 + i$. Since $Q = (0, 0)$ is the only such element, we are done. □

The test can be further rewritten as follows. Let

$$(x_m, y_m) = (1+i)^{m-1} \cdot P.$$

By our formula for the multiplication by $1+i$, the numbers x_m are given by a quadratic recursion

$$x_{m+1} = \frac{1}{2}\left(\frac{x_m}{i} + \frac{i}{x_m}\right)$$

starting with $x_1 = 5$. In this way we arrive to a version of the test alluded to in the introduction: The Fermat number F_ℓ is prime if and only if x_m is relatively prime to f_ℓ for all $m = 1, \ldots, 2^\ell - 1$ and x_{2^ℓ} is 0 modulo f_ℓ.

As an example we calculate the first few terms in this sequence and use them to test the primality of some small Fermat numbers. The sequence starts,

$$\{x_i\} = \left\{5, -\frac{12i}{5}, -\frac{169}{120}, \frac{14161i}{40560}, \ldots\right\}.$$

Modulo $f_2 = 4 + i$ this sequence becomes $\{5, 4, 1, 0\}$, thus $F_2 = 17$ is prime. Modulo $f_5 = 2^{16} + i$ we calculate $x_{32} \equiv 3436246100 \not\equiv 0 \pmod{f_5}$ thus F_5 is not prime as Euler first calculated in 1732. Of course our test does not necessarily factor the Fermat numbers as Euler did.

There are other choices for n and the starting point P of course. One can take $P = (\frac{3}{2}, \frac{1}{2})$, and $n = \frac{15}{2}$ giving $x_1 = \frac{3}{2}$ as the starting point. Because the formula is independent of n, one uses the same recurrence rule as before! It is of no computational benefit however to change the curve and starting point.

5. The curve $y^2 = x^3 + \frac{D}{4}$

Let C be the elliptic curve $y^2 = x^3 + \frac{D}{4}$. The discriminant of C is -3^3D^2. In particular C has a good reduction modulo any odd prime p not dividing $3D$. We let $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ represent the third root of unity in $\mathbb{C}$, as usual we have $\omega^2 = \overline{\omega}$. The ring $\mathbb{Z}[\omega]$ is known as the ring of Eisenstein integers which consists of $\{a + b\omega \mid a, b \in \mathbb{Z}\}$. The norm of this ring is given by $N(a + b\omega) = (a + b\omega) \cdot (\overline{a + b\omega}) = a^2 - ab + b^2$.

If $p \equiv 1 \pmod 3$ then, abusing notation, let ω denote a primitive third root of unity in the finite field $\mathbb{F}_p$. The action

$$\omega : (x, y) \to (\omega x, y)$$

is a degree three endomorphism of $C(p)$, and thus turns $C(p)$ into a $\mathbb{Z}[\omega]$-module.

Proposition 6. *Let p be an odd prime not dividing $3D$. If $p \equiv 1 \pmod 3$, let $p = \pi\overline{\pi}$ with $\pi \in \mathbb{Z}[\omega]$, and $\pi \equiv \overline{\pi} \equiv 2 \pmod 3$. Then,*

$$\left|C(p)\right| = p + 1 + \overline{\left(\frac{D}{\pi}\right)_6}\pi + \left(\frac{D}{\pi}\right)_6\overline{\pi}.$$

Proof. See [I&R, p. 305]. □

We now turn our attention to two more sets of integers. Define

$$\begin{cases} K_\ell = 3^{2^\ell} - 3^{2^{\ell-1}} + 1, \\ J_\ell = 2^{2^\ell} - 2^{2^{\ell-1}} + 1. \end{cases}$$

We have $K_\ell \equiv J_\ell \equiv 1 \pmod 3$. Setting

$$\begin{cases} k_\ell = -1 - 3^{2^{\ell-1}}\omega, \\ j_\ell = \omega + 2^{2^{\ell-1}}\overline{\omega} \end{cases}$$

we have factorizations $J_\ell = j_\ell \cdot \bar{j}_\ell$ and $K_\ell = k_\ell \cdot \bar{k}_\ell$. Note that $k_\ell \equiv j_\ell \equiv 2 \pmod 3$.

Corollary 7. *Let $\ell > 1$.*

(i) *Let $D = 1$. If K_ℓ is prime then $|C(K_\ell)| = 3^{2^\ell}$.*
(ii) *Let $D = 4n^3$. If J_ℓ is prime and $(\frac{n}{J_\ell})_2 = -1$ then $|C(J_\ell)| = 2^{2^\ell}$.*

Proof. For (i) if K_ℓ is prime then k_ℓ is an Eisenstein prime. By Proposition 6 we have, with $\pi = k_\ell$,

$$\left|C(K_\ell)\right| = K_\ell + 1 + k_\ell + \bar{k}_\ell = 3^{2^\ell}. \tag{2}$$

For (ii), if J_ℓ is prime then j_ℓ is an Eisenstein prime. Recall that 2 is a prime in $\mathbb{Z}[\omega]$. By cubic reciprocity (see [I&R]),

$$\left(\frac{2}{j_\ell}\right)_3 = \left(\frac{\omega + 2^{2^{\ell-1}}\overline{\omega}}{2}\right)_3 = \left(\frac{\omega}{2}\right)_3 = \omega.$$

Next, note that the inclusion of $\mathbb{Z}$ into $\mathbb{Z}[\omega]$ gives rise to an isomorphism of finite fields $\mathbb{Z}/(J_\ell)$ and $\mathbb{Z}[\omega]/(j_\ell)$. In particular, an integer n is a square modulo J_ℓ if and only if it is a square modulo j_ℓ. Therefore, since $D = 4n^3$ and n is not a square modulo J_ℓ, it follows that

$$\left(\frac{D}{j_\ell}\right)_6 = \left(\frac{2}{j_\ell}\right)_3 \left(\frac{n}{j_\ell}\right)_2 = -\omega.$$

Then by Proposition 6 we have,

$$\left|C(J_\ell)\right| = J_\ell + 1 + (-\overline{\omega}) j_\ell + (-\omega)\bar{j}_\ell = 2^{2^\ell}. \tag{3}$$

This proves the corollary. □

We now show that $n = 7$ satisfies the second condition of the corollary. By quadratic reciprocity we have

$$\left(\frac{7}{J_\ell}\right) = \left(\frac{J_\ell}{7}\right)(-1)^{\frac{7-1}{2}\frac{J_\ell - 1}{2}} = \left(\frac{J_\ell}{7}\right).$$

Modulo 7, 2^{2^ℓ} alternates between the values 2 and 4. Thus either $J_\ell \equiv 2 - 4 + 1 \equiv -1 \pmod 7$, or $J_\ell \equiv 4 - 2 + 1 \equiv 3 \pmod 7$. In both cases we have $(\frac{J_\ell}{7}) = -1$ thus $(\frac{7}{J_\ell}) = -1$. We get, by part (ii) of Corollary 7, that $|C(J_\ell)| = 2^{2^\ell}$ for $D = 7^3$.

6. The structure of the group $C(K_\ell)$

Recall that C is the elliptic curve $y^2 = x^3 + \frac{D}{4}$. Assume that K_ℓ is a prime number. Since $K_\ell \equiv 1 \pmod 3$ the group $C(K_\ell)$ is a $\mathbb{Z}[\omega]$-module.

Proposition 8. *Let C be the elliptic curve $y^2 = x^3 + \frac{1}{4}$. If K_ℓ is prime then*

$$C(K_\ell) \cong \mathbb{Z}[\omega]/\left(\omega - \omega^2\right)^{2^{\ell-1}}$$

as $\mathbb{Z}[\omega]$-modules.

Proof. This is proved in the same way as Proposition 4. We observe that $|C(J_\ell)| = 3^{2^\ell}$ and that $(\omega - \omega^2)$ is the unique prime ideal in $\mathbb{Z}[\omega]$ with norm equal to a power of 3 and multiplication by $\omega - \omega^2$ is a degree 3 endomorphism. □

Next, we want to find a generator of the $\mathbb{Z}[\omega]$-module $C(K_\ell)$. To this end, let C_n be the cubic twist $y^2 = nx^3 + \frac{1}{4}$. Clearly, if n is a cube, then

$$(x, y) \mapsto \left(n^{\frac{1}{3}} \cdot x, y\right)$$

gives an isomorphism between $\mathbb{Z}[\omega]$-modules $C_n(K_\ell)$ and $C(K_\ell)$. We can construct rational points on C_n by picking y and then factoring a cube out of $y^2 - \frac{1}{4}$. Trying $y = 2$ we get $x = \frac{1}{2}$ and $n = 30$. We have constructed the point $P = (\frac{1}{2}, 2)$ on the curve

$$y^2 = 30x^3 + \frac{1}{4}.$$

Of course, we must show that 30 is a cube modulo K_ℓ or, equivalently, modulo k_ℓ. Recall that 2 is a prime in $\mathbb{Z}[\omega]$. By cubic reciprocity,

$$\left(\frac{2}{k_\ell}\right)_3 = \left(\frac{-1 - 3^{2^{\ell-1}}\omega}{2}\right)_3 = \left(\frac{-1 - \omega}{2}\right)_3 = \omega^2.$$

Next, 5 is also a prime in $\mathbb{Z}[\omega]$, and $5 \equiv 2 \pmod 3$. Then by cubic reciprocity

$$\left(\frac{5}{k_\ell}\right)_3 = \left(\frac{-1 - 3^{2^{\ell-1}}\omega}{5}\right)_3 = \left(\frac{-1 - \omega}{5}\right)_3 = \left(\omega^2\right)^{\frac{5^2-1}{3}} = \omega.$$

Note that, since $K_\ell \equiv 1 \pmod 9$ for $\ell > 1$, ω is a cube modulo K_ℓ. Since $1 - \omega$ is a cube modulo k_ℓ by p. 114 in [I&R], we conclude that $-3 = (\omega - \omega^2)^2$ and 3 are cubes modulo k_ℓ:

$$\left(\frac{3}{k_\ell}\right)_3 = 1.$$

Putting these calculations together yields,

$$\left(\frac{30}{k_\ell}\right)_3 = \left(\frac{2}{k_\ell}\right)_3 \cdot \left(\frac{5}{k_\ell}\right)_3 \cdot \left(\frac{3}{k_\ell}\right)_3 = 1. \tag{4}$$

This shows that 30 is a cube modulo any prime K_ℓ.

Using the addition formula for our curve, $y^2 = nx^3 + \frac{1}{4}$ we see $(\omega - \omega^2) \cdot (x, y) = (x', y')$ where

$$\begin{cases} x' = \dfrac{1}{n}A^2 + x = -\dfrac{nx^3+1}{3nx^2}, \\ y' = -y - A(x' - \omega x) = y(\omega - \omega^2) + \dfrac{8}{3(\omega-\omega^2)} \cdot \dfrac{y^3}{y^2 - \frac{1}{4}} \end{cases} \tag{5}$$

and A is the slope of the line through the points $(\omega x, y)$ and $(\omega^2 x, -y)$, given by

$$A = \frac{2y}{(\omega - \omega^2)x}.$$

Proposition 9. *Let $\ell > 1$ be such that K_ℓ is prime. Then the rational point $P = (\frac{1}{2}, 2)$ is a generator of the $\mathbb{Z}[\omega]$-module*

$$C_{30}(K_\ell) \cong \mathbb{Z}[\omega]/(\omega - \omega^2)^{2^\ell}.$$

Proof. We must show that there is no point R in $C_{30}(K_\ell)$ such that

$$\left(\frac{1}{2}, 2\right) \equiv (\omega - \omega^2) \cdot R \pmod{K_\ell}.$$

Assume there was such a point, $R = (x, y)$. By the formula (5) for multiplication by $\omega - \omega^2$, solving for $R = (x, y)$ amounts to solving a cubic equation

$$30x^3 + 45x^2 + 1 = 0.$$

We substitute $z = \frac{1}{x}$ to get the equation,

$$z^3 + 45z + 30 = 0. \tag{6}$$

Assume that R in $C_{30}(K_\ell)$ is one solution. If $S \in C_{30}(K_\ell)$ satisfies $(\omega - \omega^2) \cdot S \equiv O \pmod{K_\ell}$, then $R + S$ is another solution. There are three such S, thus we get three distinct solutions to $(\omega - \omega^2) \cdot R \equiv P \pmod{K_\ell}$. It follows that the polynomial (6) splits in $\mathbb{F}_{K_\ell}$.

On the other hand, one can solve (6) as in [D&F]. We see $p = 45$ and $q = 30$ so that the discriminant $D = -4p^3 - 27q^2 = -3(2^3 \cdot 3^2 \cdot 5)^2$. Now this equation has a solution if and only if the value,

$$\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D} = 3^5 \cdot 5$$

is a cube *in* $\mathbb{F}_{K_\ell}$. Using our previous computations we find,

$$\left(\frac{3^5 \cdot 5}{k_\ell}\right)_3 = \left(\frac{5}{k_\ell}\right)_3 = \omega.$$

This shows that (6) does not have a root in $\mathbb{F}_{K_\ell}$. It follows that the polynomial in (6) does not actually split over $\mathbb{F}_{K_\ell}$, and so there is no solution to $(\omega - \omega^2) \cdot R \equiv P \pmod{K_\ell}$. This finishes the proof that P generates $C_{30}(K_\ell)$. □

7. Elliptic curve test for the primes K_ℓ

We now develop a test for the numbers K_ℓ using the curve $y^2 = 30x^3 + \frac{1}{4}$ and the point $P = (\frac{1}{2}, 2)$. It is more natural to state the test is in terms of Eisenstein integers. Recall that we have a factorization in $\mathbb{Z}[\omega]$.

$$K_\ell = k_\ell \cdot \bar{k}_\ell$$

where $k_\ell = -1 - 3^{2^{\ell-1}}\omega$. Now, K_ℓ is a prime integer if and only if k_ℓ is an Eisenstein prime. Note that the points of order $\omega - \omega^2$ on $y^2 = 30x^3 + \frac{1}{4}$ are

$$\left(0, \pm\frac{1}{2}\right).$$

Theorem. *Let $P = (\frac{1}{2}, 2)$ be a point on the elliptic curve C_{30}: $y^2 = 30x^3 + \frac{1}{4}$. Let $\ell > 1$. The number $K_\ell = 3^{2^\ell} - 3^{2^{\ell-1}} + 1$ is prime if and only if*

$$\left(\omega - \omega^2\right)^{2^\ell - 1} \cdot P \equiv \left(0, \pm\frac{1}{2}\right) \pmod{k_\ell}.$$

Proof. Assume the congruence holds. Suppose K_ℓ is not prime. Then there exists a prime factor p of K_ℓ such that $p < \sqrt{K_\ell}$. The prime cannot be 2, 3 or 5 so the curve has good reduction modulo p. Since p divides K_ℓ,

$$0 \equiv 3^{2^\ell} - 3^{2^{\ell-1}} + 1 \equiv x^2 - x + 1 \pmod{p}$$

which shows there is a non-trivial cube root of one mod p. This shows $p \equiv 1 \pmod 3$. Then $p = \pi\overline{\pi}$ for some Eisenstein prime π. We can assume that π divides k_ℓ. We get the congruence

$$\left(\omega - \omega^2\right)^{2^\ell - 1} \cdot P \equiv \left(0, \pm\frac{1}{2}\right) \pmod{\pi}.$$

Multiplying both sides of the congruence by $\omega - \omega^2$ yields

$$\left(\omega - \omega^2\right)^{2^\ell} \cdot P \equiv O \pmod{\pi}.$$

Thus P generates a $\mathbb{Z}[\omega]$-submodule of $C_{30}(\pi)$ isomorphic to $\mathbb{Z}[\omega]/((\omega - \omega^2)^{2^\ell})$. The order of this module is $N((\omega - \omega^2)^{2^\ell}) = 3^{2^\ell}$, so we must have

$$\left|C_{30}(\pi)\right| \geqslant 3^{2^\ell}.$$

By Hasse's estimate we also have $|C_{30}(\pi)| \leqslant (\sqrt{p}+1)^2$. Combining these with the earlier remark, $p \leqslant \sqrt{K_\ell} < 3^{2^{\ell-1}}$, we get the inequality,

$$3^{2^\ell} \leqslant \left|C_{30}(p)\right| \leqslant (\sqrt{p}+1)^2 < 3^{2^{\ell-1}} + 2\cdot 3^{2^{\ell-2}} + 1$$

which holds for no $\ell > 1$. This is a contradiction, so it must be that K_ℓ is prime.

For the other direction assume that K_ℓ is prime. By Proposition 8,

$$C_{30}(k_\ell) \cong C_{30}(K_\ell) \cong \mathbb{Z}[\omega]/\left(\left(\omega-\omega^2\right)^{2^\ell}\right),$$

and by Proposition 9 the point P generates this $\mathbb{Z}[\omega]$-module. Therefore $(\omega-\omega^2)^{2^\ell-1}\cdot P$ is an element of order $\omega-\omega^2$ and this is $(0, \frac{1}{2})$ or $(0, -\frac{1}{2})$. The theorem follows. □

We now formulate the more elegant version of this test. Define $y_1 = 2$, and recursively define

$$y_{m+1} = y_m\left(\omega-\omega^2\right) + \frac{8}{3(\omega-\omega^2)}\cdot\frac{y_m^3}{y_m^2-\frac{1}{4}}.$$

Then the number $K_\ell = 3^{2^\ell} - 3^{2^{\ell-1}} + 1$ is prime if and only if $y_m^2 - \frac{1}{4}$ is relatively prime to K_ℓ for $m = 1,\dots,2^\ell-1$ and $y_{2^\ell}^2 - \frac{1}{4}$ is zero mod K_ℓ.

8. The structure of the group $C(J_\ell)$

The curve $y^2 = x^3 + n^3$ $(D = 4n^3)$ can be rewritten as $ny^2 = x^3 + 1$ using the substitution

$$(x, y) \mapsto \left(n^{-1}x, n^{-2}y\right).$$

Let C_n denote this curve. Assume that J_ℓ is a prime number. Since $J_\ell \equiv 1 \pmod 3$, the group $C_n(J_\ell)$ is a $\mathbb{Z}[\omega]$-module.

Proposition 10. *If J_ℓ is prime and $(\frac{n}{J_\ell})_2 = -1$ then*

$$C_n(J_\ell) \cong \mathbb{Z}[\omega]/\left(2^{2^{\ell-1}}\right)$$

as $\mathbb{Z}[\omega]$-modules.

Proof. This is proved in the same way as Proposition 4, using that $|C_n(J_\ell)| = 2^{2^\ell}$ and observing that (2) is the unique prime ideal in $\mathbb{Z}[\omega]$ with norm equal to a power of 2 and multiplication by 2 is a degree 4 endomorphism. □

For the primes J_ℓ we will need to make use of the duplication formula on our curve. The slope of the tangent line to (x, y) on the curve $ny^2 = x^3 + 1$ is defined to be

$$A = \frac{dy}{dx} = \frac{3x^2}{2ny}.$$

One now checks that the duplication formula takes the shape $2 \cdot (x, y) = (x', y')$ where

$$\begin{cases} x' = nA^2 - 2x = \dfrac{x^4 - 8x}{4(x^3 + 1)}, \\ y' = -y - A(x' - x). \end{cases} \tag{7}$$

We know that $n = 7$ is not a square modulo all primes J_ℓ. In particular, Proposition 10 holds for C_7. This curve has a rational point $P = (3, 2)$.

Proposition 11. *Let $\ell > 1$ be such that J_ℓ is prime. Then the rational point $P = (3, 2)$ is a generator of the $\mathbb{Z}[\omega]$-module*

$$C_7(J_\ell) \cong \mathbb{Z}[\omega]/\left(2^{2^{\ell-1}}\right).$$

Proof. It suffices to show that the equation

$$P = (3, 2) \equiv 2 \cdot R \pmod{J_\ell}$$

has no solution in $C_7(J_\ell)$. By the duplication formula (7), solving for $R = (x, y)$ amounts to solving a quartic equation

$$x^4 - 12x^3 - 8x - 12 = 0. \tag{8}$$

Assume that R in $C(J_\ell)$ is one solution. Now if $S \in C(J_\ell)$ satisfies $2 \cdot S \equiv O \pmod{J_\ell}$, then we have $R + S$ is another solution. There are four such S, thus we get four distinct solutions to $2 \cdot R \equiv P \pmod{J_\ell}$ in $C_7(J_\ell)$. It follows that the polynomial in (8) splits in $\mathbb{F}_{J_\ell}$.

On the other hand, recall that $(\frac{7}{J_\ell}) = -1$, thus $\mathbb{F}_{J_\ell}[\sqrt{7}]$ is a degree 2 extension. In this extension we have the (tricky) factorization,

$$x^4 - 12x^3 - 8x - 12 = \left(x^2 - 2(3 + \sqrt{7})x - 2(2 + \sqrt{7})\right) \cdot \left(x^2 - 2(3 - \sqrt{7})x - 2(2 - \sqrt{7})\right).$$

If x_1, x_2 were the two roots of the first term in the right-hand side of this equation then we would have $x_1 + x_2 = 2(3 + \sqrt{7})$, and as such we see one of x_1, x_2 is not an element of $\mathbb{F}_{J_\ell}$. It follows that the polynomial in (8) does not actually split over $\mathbb{F}_{J_\ell}$, and so there is no solution to $2 \cdot R \equiv P \pmod{J_\ell}$. This finishes the proof that P generates $C_7(J_\ell)$. □

9. Elliptic curve test for the primes J_ℓ

Finally, we develop a test for the numbers J_ℓ using the curve $7y^2 = x^3 + 1$ and the point $P = (3, 2)$. Again, it is more natural to state the test is in terms of Eisenstein integers. Recall that we have a factorization in $\mathbb{Z}[\omega]$.

$$J_\ell = j_\ell \cdot \bar{j}_\ell$$

where $j_\ell = \omega + 2^{2^{\ell-1}}\bar{\omega}$. Now, J_ℓ is a prime integer if and only if j_ℓ is an Eisenstein prime. Note that the points of order 2 on $7y^2 = x^3 + 1$ are of the form

$$\left(-\omega^j, 0\right).$$

Theorem. *Let $P = (3, 2)$ be a point on the elliptic curve C_7: $7y^2 = x^3 + 1$. Let $\ell > 1$. The number $J_\ell = 2^{2^\ell} - 2^{2^{\ell-1}} + 1$ is prime if and only if*

$$2^{2^{\ell-1}-1} \cdot P \equiv \left(-\omega^j, 0\right) \pmod{j_\ell}.$$

Proof. Assume the congruence is true. Suppose J_ℓ is not prime. Then there exists a prime factor p of J_ℓ such that $p < \sqrt{J_\ell}$. The prime cannot be 3, nor 7 so the curve has good reduction modulo p. Since p divides J_ℓ,

$$0 \equiv 2^{2^\ell} - 2^{2^{\ell-1}} + 1 \equiv x^2 - x + 1 \pmod{p}$$

which shows there is a non-trivial cube root of one mod p. This shows $p \equiv 1 \pmod 3$ and we can write $p = \pi\overline{\pi}$ for an Eisenstein prime π. Without any loss of generality, we can assume that π divides j_ℓ. By assumption, we also get the congruence

$$2^{2^{\ell-1}-1} \cdot P \equiv \left(-\omega^j, 0\right) \pmod{\pi}.$$

Multiplying both sides of the congruence by 2 yields

$$2^{2^{\ell-1}} \cdot P \equiv O \pmod{p}.$$

Thus P generates a $\mathbb{Z}[\omega]$-submodule of $C_7(\pi)$ isomorphic to $\mathbb{Z}[\omega]/(2^{2^{\ell-1}})$. The order of this module is $N(2^{2^{\ell-1}}) = 2^{2^\ell}$, so we must have

$$\left|C_7(\pi)\right| \geqslant 2^{2^\ell}.$$

By Hasse's estimate we also have $|C_7(\pi)| \leqslant (\sqrt{p}+1)^2$. Combining these with the earlier remark, $p \leqslant \sqrt{J_\ell} < 2^{2^{\ell-1}}$, we get the awkward inequality,

$$2^{2^\ell} \leqslant \left|C_7(\pi)\right| \leqslant (\sqrt{p}+1)^2 < 2^{2^{\ell-1}} + 2 \cdot 2^{2^{\ell-2}} + 1$$

which holds for no $\ell > 1$. This is a contradiction, so it must be that J_ℓ is prime.

For the other direction assume that J_ℓ is prime. By Proposition 10,

$$C_7(j_\ell) \cong C_7(J_\ell) \cong \mathbb{Z}[\omega]/\left(2^{2^{\ell-1}}\right),$$

and by Proposition 11 the point P generates this $\mathbb{Z}[\omega]$-module. It follows that $2^{2^{\ell-1}-1} \cdot P$ is an element of order 2, hence of the form $(-\omega^j, 0)$. The theorem follows. □

We can reformulate this test in a similar way to the first test *without* even using the Eisenstein integers. Define $x_1 = 3$, and then recursively define

$$x_{m+1} = \frac{x_m^4 - 8x_m}{4(x_m^3 + 1)}.$$

Then the number $J_\ell = 2^{2^\ell} - 2^{2^{\ell-1}} + 1$ is prime if and only if $x_m^3 + 1$ is relatively prime to J_ℓ for $n = 1, \ldots, 2^{\ell-1} - 1$ and $x_{2^{\ell-1}}^3 + 1$ is zero mod J_ℓ.

Acknowledgments

This paper is motivated by a short note by Dick Gross [Gross] in which an elliptic curve test for Mersenne numbers is developed. We would like to thank the referee for a suggestion regarding organization of the material. The first author was supported by NSF VIGRE grant (REU, Research Experience for Undergraduates) during his stay at the University of Utah. The second author is supported by NSF grant DMS 0551846.

References

[D&F] David S. Dummit, Richard M. Foote, Abstract Algebra, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. 630–632.

[Gross] Benedict H. Gross, An elliptic curve test for Mersenne primes, J. Number Theory 110 (1) (2005) 114–119.

[I&R] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, second ed., Grad. Texts in Math., vol. 84, Springer-Verlag, New York, 1990.

Further reading

[Goldwasser] Shafi Goldwasser, Joe Kilian, Primality testing using elliptic curves, J. ACM 46 (4) (1999) 450–472.

[R&S] Karl Rubin, Alice Silverberg, Ranks of elliptic curves, Bull. Amer. Math. Soc. (N.S.) 39 (4) (2002) 455–474 (electronic).