rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Primetesting using Elliptic Curves

Bacheloronderzoek Wiskunde

7 Februari 2015

Student: J. Hamersma

Eerste Begeleider: J. Top

Tweede Begeleider: A. E. Sterk

1 Introduction

Mathematics in general has interested me for as long as I can remember. Playing with numbers and puzzling intrigued me. After high school I decided to study Mathematics at the Rijksuniversiteit Groningen. After following multiple courses over the years, I had to decide on a subject for this paper. After following courses on statistics and geometry, I realized I didn't like those subjects too much. Chaos theory and Linear Algebra on the other hand I did find interesting. Since I had already done a project on Chaos theory, I came across a subject on prime numbers led by Professor Top. Unfortunately the subject was outdated, but Professor Top showed me an article by B.H. Gross which I could use as a basis for my paper.

Prime numbers and prime tests belong to the part of Mathematics called Number Theory. While studying numbers and their qualities goes back hundreds of years, there is still much to explore and discover in this area. There are a lot of theorems stated about numbers that haven't been proven or disproven yet, so it is an interesting field for new mathematicians. The Lucas-Lehmer test for Mersenne numbers is a remarkably efficient test to check whether a Mersenne number $M_n = 2^n - 1$ is prime or not. Within Mathematics the Mersenne primes are well-known and also an active area of research.

B. H. Gross developed a different test for the same group of numbers, using properties from elliptic curves. By doubling a point on an elliptic curve a certain number of times, Gross' test determines whether a Mersenne number is prime or not. While the calculations involved are slightly more complicated then the Lucas-Lehmer test and therefore Gross' test being less efficient, it is useful as a basis for more prime tests using elliptic curves. Gross' idea can be transfered to say something about other groups of numbers as well.

Using Gross' test as a guideline, I was able to develop two new tests using elliptic curves. The first test determines whether a number $3 \cdot 8^n - 1$ is prime or not and the second one determines whether $12 \cdot 8^n - 1$ is prime or not. Using a different elliptic curve and a different starting point, doubling a point over the elliptic curve can show whether such a number is prime or not. These tests can also be implemented, but since the main focus of this paper was to understand the other tests and show the new tests, the calculations done with them are modest. However, the results that were found during the study will be mentioned.

I like to thank Professor J. Top for his guidance and help during this project. Without his help I wouldn't have come across the subject, let alone been able to find these new tests. Also several proofs and suggestions became clearer after talking about them with Professor Top. His revisions and comments helped me understand the subject better and gave me a wider understanding of several mathematical ideas. I also want to thank Professor Sterk for his revisions and comments on the paper. It is always useful to hear a new opinion or idea.

2 Quadratic Reciprocity

Throughout the rest of this paper frequently the question will return whether a certain prime number p is a square modulo a prime q and similar related questions. While for some numbers some basic algebra can go a long way, in order to keep the rest of the paper as clean as possible quadratic reciprocity will be introduced first. With this knowledge, other statements later can be proven quite clean and fast, making the paper better to read.

Lemma 2.1

Suppose q is an odd prime. If $a \not\equiv 0 \bmod q$ is a square mod q, $a^{\frac{q-1}{2}} \equiv 1 \bmod q$ and $a^{\frac{q-1}{2}} \equiv -1 \bmod q$ if a is not a square mod q.

Proof of Lemma 2.1

Following the proof found on [1]. Suppose $a \equiv x^2 \bmod q$. By Fermat $x^q \equiv x \bmod q$, so $x^{q-1} \equiv 1 \bmod q$. Hence $a^{\frac{q-1}{2}} \equiv x^{q-1} \equiv 1 \bmod q$ by Fermat again. Assume now $a^{\frac{q-1}{2}} \equiv 1 \bmod q$. Let r be a primitive root modulo q, so we have $amodq \equiv r^j$ for some j. Then $r^{j(\frac{q-1}{2})} \equiv 1 \bmod q$. By definition r has order $q-1$, so $q-1|j(\frac{q-1}{2})$, so $j \cdot \frac{q-1}{2} = (q-1) \cdot b$ for some b. Dividing by $\frac{q-1}{2}$ leads to $j = 2b$. Hence $b = \frac{j}{2}$. Then $(r^b)^2 \equiv r^j \equiv a \bmod q$. Hence a is a square mod q. If a is not a square, $a^{q-1} \equiv 1 \bmod q$, but by the previous reasoning, $a^{\frac{q-1}{2}}$ can't be equivalent to 1 mod q, since $a^{q-1} \equiv 1 \bmod q$ implies $a^{\frac{q-1}{2}} \equiv \pm 1 \bmod q$, so $a^{\frac{q-1}{2}} \equiv -1 \bmod q$. ■

Notice that this means for $a \equiv -1 \bmod q$, we have $(-1)^{\frac{q-1}{2}} \equiv 1$ if $q \equiv 1 \bmod 4$ and $(-1)^{\frac{q-1}{2}} \equiv -1$ if $q \equiv 3 \bmod 4$. For the paper it is relevant to see that -1 is not a square mod q if $q \equiv 3 \bmod 4$. One final observation considering a pair $\{-x, x\}$ is, that when looking modulo $p \equiv 3 \bmod 4$, either x or $-x$ is a square, since $x = -1 \cdot (-x)$ and -1 is not a square mod p. So if x is not a square, $-x$ has to be a square and vice versa. Considering a primitive root, every square has an even exponent and every non-square an odd exponent, so multiplying two non-squares results in a square and multiplying a non-square with a square results in a non-square.

Definition The Legendre symbol is used to state whether a number a is a square mod q. The value of the Legendre symbol $\left(\frac{a}{q}\right)$ depends on whether a is a square modulo p or not in the following way:

$\left(\frac{a}{q}\right) = 0$ if $a \equiv 0 \bmod q$.
$\left(\frac{a}{q}\right) = +1$ if a is a square mod q.
$\left(\frac{a}{q}\right) = -1$ if a is not a square mod q.

With the legendre symbol, we can restate Lemma 2.1 in the following way: For any $a \in \mathbb{Z}$ and any odd prime q, $a^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right) \bmod q$.

Quadratic Reciprocity

The law of quadratic reciprocity is useful to check squares mod p if p is large. Before stating and proving the law, one Lemma will be necessary. This complete section will follow [2].

Lemma 2.2

$\left(\frac{q}{p}\right) = (-1)^{\sum_u \lfloor \frac{qu}{p} \rfloor}$, where $\lfloor x \rfloor$ denotes the floor function and u ranges over the even integers $u = 2, 4, .., p-1$.

Proof of Lemma 2.2

For an even integer u in the range $1 \leq u \leq p-1$, denote $r(u)$ as the least positive residue of qu mod p. Consider $(-1)^{r(u)}r(u)$ again as least positive residue mod p. So for even $r(u)$ it stays the same and for odd $r(u)$ we get $-r(u)+p$. This leads to $\frac{p-1}{2}$ even numbers in the range $(1..p-1)$. They are all distinct, since $r(u) \equiv r(t)$ mod p leads to $qu \equiv qt$ mod p and after dividing by q leads to $u \equiv t$ mod p, $-r(u)+p \equiv -r(t)+p$ mod p leads to $u \equiv t$ mod p similarly and last $-r(u)+p \equiv r(t)$ mod p, means $-qu+p \equiv qt$ mod p or $-u \equiv t$ mod p which is not possible since u and t are both assumed even in $(1..p-1)$ and p is odd. Since they are different and there are exactly $\frac{p-1}{2}$ of them, they must be a rearrangement of the even integers $2, 4, .., p-1$. Multiplying both arrangements we obtain $(-1)^{r(2)}2q \cdot (-1)^{r(4)}4q \cdot \cdots (-1)^{r(p-1)}(p-1)q \equiv 2 \cdot 4 \cdots (p-1)$ mod p. Since none of $2, 4, .., p-1$ are divisible by p, we can divide them out and rearrange to get: $q^{\frac{p-1}{2}} \equiv (-1)^{r(2)+r(4)+..+r(p-1)}$ mod p. On the other hand, by the definitions of $r(u)$ and the floor function, we have $\frac{qu}{p} = \lfloor \frac{qu}{p} \rfloor + \frac{r(u)}{p}$. Now, since p is odd and u is even, $\lfloor \frac{qu}{p} \rfloor$ and $r(u)$ are congruent mod 2. Combining these results, we get to the Lemma: $\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}} \equiv (-1)^{\sum_u \lfloor \frac{qu}{p} \rfloor}$ mod p. ■

The law of Quadratic Reciprocity

If p, q are both distinct odd primes and at least one $\equiv 1 \bmod 4$, $p \equiv x^2 \bmod q$ has a solution if and only if $q \equiv x^2 \bmod p$ has a solution.

If p, q are both distinct odd primes and $p \equiv q \equiv 3 \bmod 4$, $p \equiv x^2 \bmod q$ has no solution if and only if $q \equiv x^2 \bmod p$ has a solution and vice versa.

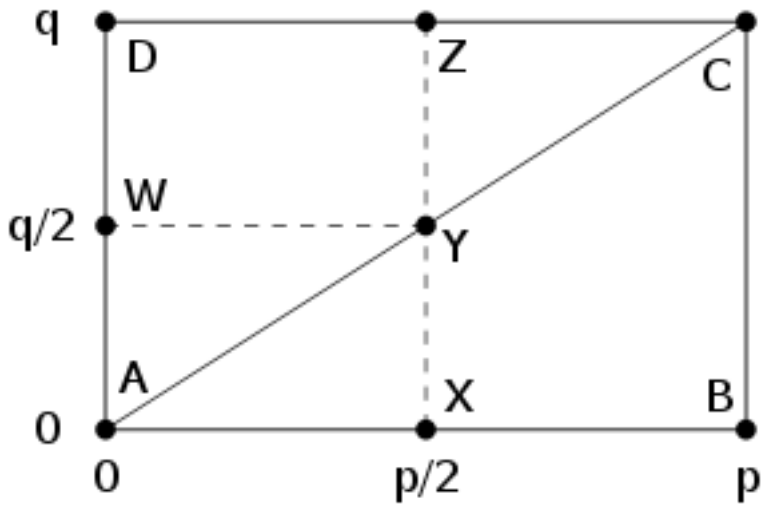
An alternative way to state this using the Legendre symbol is:

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Proof of Law of Quadratic Reciprocity

While there are multiple ways to prove quadratic reciprocity, the proof given here will be following [2].

Let p and q be odd primes. Consider the following diagram, dividing the rectangle $((0,0),(p,0),(0,q),(p,q))$ into several regions.



The sum $\sum_u \lfloor \frac{qu}{p} \rfloor$ counts the number of lattice points with even x-coordinate in the interior of the triangle ABC. Since each column has $q-1$ points, the number of lattice points with even x-coordinate inside the region $BCYX$ is the same mod 2 as the number of such points inside the region CZY. By flip-

ping the diagram in both axes, the number of points with even x-coordinate inside CZY is the same as the number of points inside AXY having odd x-coordinates. The conclusion is that $\left(\frac{q}{p}\right) = (-1)^{\alpha}$, where α is the total number of lattice points inside AYX. Switching p and q, the same reasoning shows $\left(\frac{p}{q}\right) = (-1)^{\beta}$, where β is the number of lattice points inside WYA. Finally, there can't be any lattice points on the diagonal AY, since any point (a, b) on that diagonal satisfies $b = \frac{q}{p}a$ and since p and q are distinct odd primes, any such point lies outside $AXYW$. The total number of points inside $AXYW$ is $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Combining these statements, we get the law of quadratic reciprocity: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha+\beta} = (-1)^{\frac{(p-1)(q-1)}{4}}$. ■

This gives a general theorem of quadratic reciprocity. In order to keep the rest of the paper as clean as possible, all relevant cases will be evaluated here.

2.1 Specific Cases of Quadratic Reciprocity

While the law of Quadratic Reciprocity is very general, only certain specific cases will be used in this paper. Instead of showing the relations when they arise, all necessary quadratic reciprocity related properties will be proven here.

Case 1

Suppose $M_n = 2^n - 1$ is prime with $n > 3$ odd. $2^n \equiv 1 \bmod M_n$, so $2^{n+1} \equiv 2 \bmod M_n$. Since n is odd, $(2^{\frac{n+1}{2}})^2 \equiv 2 \bmod M_n$, so 2 is a square mod M_n. Then by Lemma 2.1, $2^{\frac{M_n-1}{2}} \equiv 1 \bmod M_n$.

Case 2

Suppose $M_n = 2^n - 1$ is prime with $n \geq 3$. Then $M_n \equiv 3 \bmod 4$. If $2^n - 1$ is prime, then $2^n - 1 \equiv 1 \bmod 3$, since $2^n - 1$ is not divisible by 3 if it's prime, nor is 2^n. Hence $2^n - 2 \equiv 0 \bmod 3$ and thus $2^n - 1 \equiv 1 \bmod 3$. Since 1 is a square mod 3 ($x = -1$), 3 is not a square mod M_n by quadratic reciprocity. Consequently by Lemma 2.1, $3^{\frac{M_n-1}{2}} \equiv -1 \bmod M_n$.

As a consequence of 3 not being a square mod M_n, $12 = 2 \cdot 2 \cdot 3$ is also not a square mod M_n.

Case 3

Suppose $H_n = 3 \cdot 8^n - 1$ is prime with $n > 0$. Then $H_n \equiv 7 \equiv 3 \bmod 4$. $H_n = 3 \cdot 8^n - 1 \equiv 3 \cdot 1^n - 1 \equiv 2 \bmod 7$. $3^2 \equiv 2 \bmod 7$, so H_n is a square mod 7. Then by quadratic reciprocity, 7 is not a square mod H_n.

Case 4

Suppose $H_n = 12 \cdot 8^n - 1$ is prime with $n > 0$. Then $H_n \equiv 7 \equiv 3 \bmod 4$. $H_n = 12 \cdot 8^n - 1 \equiv -2 \cdot 1^n - 1 \equiv 4 \bmod 7$. $2^2 \equiv 4 \bmod 7$, so H_n is a square mod 7. By quadratic reciprocity, 7 is not a square mod H_n.

Using the notion of quadratic reciprocity we can now look at the actual tests for testing prime numbers. Wherever necessary the specific cases here will be referred to when making a statement about them.

3 Lucas-Lehmer primality test for Mersenne primes

According to [3] Édouard Lucas developed a test in 1856 to check if so-called Mersenne numbers, $M_n = 2^n - 1$ are prime or not. He further improved the test in 1878 and Derrick Henry Lehmer further improved it in the 1930s. In this chapter, the test will be proven as a basis for other tests later derived as well as for the completeness of this paper. Before stating the actual test, one small algebraic derivation is useful.

Lemma 3.1 Let $a_0 = 4$ and define iteratively $a_{n+1} = a_n^2 - 2$. Then $a_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$

Proof of Lemma 3.1

Basis. Take $n = 0$, then $a_0 = (2+\sqrt{3}) + (2-\sqrt{3}) = 4$.

Inductive step. Suppose $a_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$.
Then

$$\begin{aligned} a_{n+1} &= a_n^2 - 2 \\ &= ((2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n})^2 - 2 \\ &= (2+\sqrt{3})^{2^{n+1}} + (2-\sqrt{3})^{2^{n+1}} + 2 \cdot (2+\sqrt{3})^{2^n} \cdot (2-\sqrt{3})^{2^n} - 2 \\ &= (2+\sqrt{3})^{2^{n+1}} + (2-\sqrt{3})^{2^{n+1}} \end{aligned}$$

■

With this Lemma, we can now prove the Lucas-Lehmer test for Mersenne numbers without introducing many new concepts. The reason the exponent of the Mersenne number is taken odd, comes from the equality $2^{2p}-1 = (2^p+1)(2^p-1)$, hence these numbers are never prime.

The Lucas-Lehmer test for Mersenne numbers (LL) Given an odd number n and corresponding Mersenne number $M_n = 2^n - 1$, M_n is prime if and only if $a_{n-2} \equiv 0 \bmod M_n$, where $a_0 = 4$ and $a_{n+1} = a_n^2 - 2 \bmod M_n$.

Proof of sufficiency of LL

Extending [4]. Given $a_{n-2} \equiv 0 \bmod M_n$, there exists some real integer R such that $R \cdot M_n = a_{n-2} = (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}}$. Multiplying with $(2+\sqrt{3})^{2^{n-2}}$ gives

$$R \cdot M_n \cdot (2+\sqrt{3})^{2^{n-2}} - 1 = (2+\sqrt{3})^{2^{n-1}} \tag{1}$$

Suppose M_n is composite and let q be a prime divisor of M_n with $q^2 \leq M_n$. Consider the collection

$$\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}/\{q \cdot (a + b\sqrt{3}) \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{3}]/(M_n)$$

Combined with the standard addition:

$$(a + b\sqrt{3} \bmod (q)) + (c + d\sqrt{3} \bmod (q)) = (a + c) + (b + d)\sqrt{3} \bmod (q)$$

and standard multiplication:

$$(a + b\sqrt{3} \bmod (q)) \cdot (c + d\sqrt{3} \bmod (q)) = (ac + 3bd) + (bc + ad)\sqrt{3} \bmod (q)$$

this collection is a Ring G with q^2 elements (q options for a and q options for b), whose elements will be denoted by $a + b\sqrt{3} \bmod (q)$. Define G^* the group of units of G. The number of elements in G^* is at most $q^2 - 1$, since $(0 + 0\sqrt{3})$ is not invertible. The order of an element in G^* is consequently at most $q^2 - 1 \leq M_n - 1$. Furthermore, $(2 + \sqrt{3}) \bmod (q) \in G^*$, since $(2 + \sqrt{3} \bmod (q)) \cdot (2 - \sqrt{3} \bmod (q)) \equiv 1 \bmod (q)$.

From **equation 1**: $(2 + \sqrt{3})^{2^{n-1}} \equiv -1 \bmod (q) \not\equiv 1 \bmod (q)$ since $q \neq 2$. Then $(2 + \sqrt{3})^{2^n} \equiv 1 \bmod (q)$, so the order of $(2 + \sqrt{3})$ divides 2^n but not 2^{n-1}, so the order of $(2 + \sqrt{3})$ is 2^n. However, an element's order was at most $M_n - 1 = 2^n - 2$, which leads to the desired contradiction. Hence M_n is not composite and therefore prime. ■

Proof of necessity of LL

Notice that $(2+\sqrt{3}) = \frac{(6+2\cdot\sqrt{3})^2}{24}$ and $(6+2\cdot\sqrt{3})^{M_n} \equiv 6+2\cdot 3^{(M_n-1)/2}\cdot\sqrt{3}$ mod M_n. Then combined with Case 1 and Case 2 from Chapter 2:

$$\begin{aligned}
a_{n-2} &\equiv (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \\
&\equiv ((2+\sqrt{3})^{2^{n-1}} + 1)\cdot(2-\sqrt{3})^{2^{n-2}}) \\
&\equiv (\frac{(6+2\cdot\sqrt{3})^{(M_n+1)/2}}{24^{(M_n+1)/2}} + 1)\cdot(2-\sqrt{3})^{2^{n-2}}) \\
&\equiv (\frac{(6-2\cdot\sqrt{3})\cdot(6+2\cdot\sqrt{3})}{24\cdot(2^{(M_n-1)/2})^3\cdot(3^{(M_n-1)/2})} + 1)\cdot(2-\sqrt{3})^{2^{n-2}}) \\
&\equiv (\frac{24}{24\cdot(-1)^3\cdot 1} + 1)\cdot(2-\sqrt{3})^{2^{n-2}}) \\
&\equiv 0 \text{ mod } M_n
\end{aligned}$$

Note that 2 mod M_n, 3 mod M_n and 24 mod M_n are units in $\mathbb{Z}[\sqrt{3}]/(M_n)$. which proves the necessity. ■

With the Lucas-Lehmer test it is relatively simple and quick to test whether a number $M_n = 2^n - 1$ is prime or not. Since the iterative step is quite clean (one squaring and one subtraction), the total amount of computations necessary doesn't explode and therefore it is rather efficient. It is not the only test derived for Mersenne numbers though. While the other test discussed in this paper is less efficient, it is important for the test derived later for different numbers to show what it is based on and to give credit to B. H. Gross' article [5]. Before describing the actual tests, some general statements and knowledge about elliptic curves is necessary.

4 Elliptic Curves

Elliptic curves are equations of the form $y^2 = x^3 + \alpha x + \beta$. Furthermore to eliminate cusps, self-intersections and isolated points, we require $4\alpha^3 + 27b^2 \neq 0$ and we assume the field involved has characteristic different from 2 or 3. Adding a point "at infinity" named $\mathbf{O}$, we can construct an addition $+$ on the curve. This point is also considered to be the identity point for the addition. So first of all, if $P = (x, y)$, then $P+\mathbf{O} = P$, even if $P = \mathbf{O}$. Second, if $P_1 = (x, y)$ and $P_2 = (x, -y)$, then $P_1+P_2 = \mathbf{O}$. Lastly, given any two points on the elliptic curve, the result of adding these points is defined to be the point (x, y) whose corresponding inverse $(x, -y)$ is the third intersection of the straight line through the first two points and the elliptic curve. If the initial two points are the same, the tangent line in this point determines the third intersection and thus the inverse of the result. To simplify this notion, we calculate doubling a point. Note that throughout the rest of the paper $2P$ means $P+P$ and $3P = P+P+P$.

Lemma 4.1

Doubling a point $P \to 2P$ on the elliptic curve $y^2 = x^3 + \alpha x + \beta$ takes the x-coordinate of P from x to $\frac{(x^2-\alpha)^2-8\ \beta x}{(4\cdot(x^3+\alpha x+\beta))}$.

Proof of Lemma 4.1

Simplification of [6]. The slope of the tangent line to the elliptic curve through the point $P = (x_1, y_1)$ with $y_1 \neq 0$ is $m = \frac{3x_1^2+\alpha}{2y_1}$, resulting in the tangent line $y = mx + b$. Substituting this in $y^2 = x^3 + \alpha x + \ \beta$ gives $x^3 - m^2x^2 + (\alpha - 2mb)x + (\beta - b^2) = 0$. P is a double solution to this equation, so we look for x_2 such that $x^3 - m^2x^2 + (\alpha - 2mb)x + (\beta - b^2) = (x - x_1)^2(x - x_2)$. Expanding the right side gives $x^3 + (-2x_1 - x_2)x^2 + (x_1^2 + 2x_1x_2) - x_1^2x_2$. Equating the coefficient of x^2 leads to

$$\begin{aligned}
x_2 &= m^2 - 2x_1 \\
&= (\frac{3x_1^2 + \alpha}{2y_1})^2 - 2x_1 \\
&= \frac{9x_1^4 + 6\alpha x_1^2 + \alpha^2 - 8x_1y_1^2}{4y_1^2} \\
&= \frac{9x_1^4 + 6\alpha x_1^2 + \alpha^2 - (8x_1^4 + 8\alpha x_1^2 + 8\beta x_1)}{4 \cdot (x_1^3 + \alpha x_1 + \beta)} \\
&= \frac{x_1^4 + (6-8)\alpha x_1^2 - 8\beta x_1 + \alpha^2}{4 \cdot x_1^3 + \alpha x_1 + \beta} \\
&= \frac{(x_1^2 - \alpha)^2 - 8\beta x_1}{(4 \cdot (x_1^3 + \alpha x_1 + \beta))}
\end{aligned}$$

■

In particular for two elliptic curves:

1) $y^2 = x^3 - 12x$, doubling a point P takes its x-coordinate from x to $\frac{(x^2+12)^2}{4x(x^2-12)}$ and

2) $y^2 = x^3 - 7^3$, doubling a point P takes its x-coordinate from x to $\frac{x^4+8\cdot 7^3 x}{4\cdot(x^3-7^3)}$

4.1 The number of points on the elliptic curve

In general it makes no real sense to talk about the number of points on an elliptic curve, since there may be infinitely many. This changes however if we look at an elliptic curve over a finite field. If p is prime, then $\mathbb{F}_p$ is a finite field of p elements. When looking at an elliptic curve over such a field, the amount of points could range from 1 to $2p + 1$, considering the point at infinity. While there are certain theorems that further limit these ranges, for the purpose of

this paper, only a few specific cases are interesting and for these cases the exact number of elements can be shown.

Lemma 4.2

Let $q = p^f, p$ prime. Suppose that $q \equiv 3 \bmod 4$. Then there are $q+1$ points on the elliptic curve $y^2 = x^3 - \alpha x$ over $\mathbb{F}_q$, for any $\alpha \neq 0 \in \mathbb{F}_q$.

Proof of Lemma 4.2

This proof will follow the proof found in [7]. There are two similar cases to be considered.

Case I: α is a square mod q. Suppose $\alpha = n^2$ for some n. Then there are four points of order 1 or 2; the point at infinity, $(0,0)$ and $(\pm n, 0)$. We can then arrange the remaining $q-3$ possible $x \neq 0, n, -n$ in $\frac{q-3}{2}$ pairs $\{x, -x\}$. Since $f(x) = x^3 - \alpha x$ is an odd function, we have $f(-x) = -f(x)$. Since $q \equiv 3 \bmod 4$, it follows that -1 is not a square in $\mathbb{F}_q$. Hence either $f(-x)$ or $f(x)$ is a square, so we have either $(x, \pm\sqrt{f(x)})$ or $(-x, \pm\sqrt{f(-x)})$. So each pair leads to 2 points on the curve, for $\frac{q-3}{2} \cdot 2 = q-3$ points total. Together with the four points of order 2, this gives the desired number of points $q+1$.

Case II: α is not a square mod q. In this case, there are two points of order 1 or 2; the point at infinity and $(0,0)$. We arrange the remaining $q-1$ possible $x \neq 0$ in $\frac{q-1}{2}$ pairs ($x = \pm n$ are added here). Same reasoning as Case I we have $q-1$ points together with the point at infinity and $(0,0)$ for $q+1$ total points. ■

One specific case of this is the elliptic curve $y^2 = x^3 - 12x$ over $\mathbb{F}_{M_n}$ with $M_n = 2^n - 1$ assuming M_n prime. Then $12 \not\equiv 0 \bmod M_n$ and $M_n \equiv 3 \bmod 4$, so the number of points on this curve is then $M_n + 1 = 2^n$.

Lemma 4.3

Suppose $q = p^f$, with p an odd prime and $q \equiv 2 \bmod 3$. Then there are $q+1$ points on the elliptic curve $y^2 = x^3 + \beta$ over $\mathbb{F}_q$.

Proof of Lemma 4.3

If p is an odd prime and $q \equiv 2 \bmod 3$, then $(a^{\frac{2q-1}{3}})^3 \equiv a \bmod q$, so the map $x \mapsto x^3$ defines an onto (and thus one-to-one) map from the finite field $\mathbb{F}_q$ to itself. So for each possible y, we have $y^2 - \beta = x^3$ for a unique $x \in \mathbb{F}_q$. There are q possible y, plus the point at infinity, so there are $q+1$ points on the elliptic curve. [8] ■

Note that $H_n = 3 \cdot 2^n - 1 \equiv 2 \bmod 3$, so if H_n is an odd prime, $y^2 = x^3 + \beta$ has $3 \cdot 2^n$ points over $\mathbb{F}_{H_n}$.

4.2 Divisibility by 2

With the notion of addition and looking at an elliptic curve over a finite field, it is useful to know whether a point is the result of the doubling of a point or not. If it is, we call it divisible by 2. We consider two cases:

Remark 4.1 $y^2 = x^3 + \alpha x$. Doubling a point takes its x-coordinate from x to $\frac{(x^2-\alpha)^2}{4x(x^2+\alpha)} = \frac{(x^2-\alpha)^2}{2^2y^2}$. So if a point $P = Q + Q = 2Q$, then the x-coordinate of P has to be a square. Specifically from Case 1 of Chapter 2, 2 is a square mod M_n ($M_n = 2^n - 1$ prime), so by Lemma 2.1, -2 is not a square mod M_n. Hence the point (-2,4) on the elliptic curve $y^2 = x^3 - 12x$ over M_n is not divisible by 2.

Remark 4.2 $y^2 = x^3 - 7^3$. Define $\xi = x - 7$, then we can also write $y^2 = (\xi + 7)^3 - 7^3 = \xi^3 + 21\xi^2 + 147\xi$. While not having explicitly derived in the point doubling formula, a similar derivation can be done for this type of function. A complete derivation of this can be found in [9]. The result is that on an elliptic curve of the shape $y^2 = x^3 + \alpha x^2 + \beta x$ doubling a point takes its x-coordinate to a square, so a point is not divisible by 2, if its x-coordinate is not a square. However, our elliptic curve is translated by 7, so for the elliptic curve $y^2 = x^3 - 7^3$, a point $P = (x, y)$ is not divisible by 2 if $x - 7$ is not a square. Specifically considering mod $H_n = 3 \cdot 8^n - 1$ or mod $H_n = 12 \cdot 8^n - 1$, 7 is not a square (Case 3 and 4 of chapter 2) and thus the point $(14, 49)$ on $y^2 = x^3 - 7^3$ over $\mathbb{F}_{H_n}$ is not divisible by 2.

4.3 Order of points

One last notion about elliptic curves is the how many points have a certain order or what order a certain point has. Some basic knowledge and lemmas about the order of elements are assumed to be known. The following remarks are not particularly difficult, but useful to notice nonetheless. First of all, due to the way addition is defined, a point has order 2 if and only if its y-coordinate $= 0$. This comes from $2P = \mathbf{O}$ means $P = (x, y) = -P = (x, -y)$ which leads to $P = (x, 0)$. Notice that since $\mathbf{O} + \mathbf{O} = \mathbf{O}$ we define the order of $\mathbf{O}$ to be equal to 1. Now observe the following remarks.

Remark 4.3 The only point of order 2 on the elliptic curve $y^2 = x^3 - 12x$ over $\mathbb{F}_{M_n}$ with $M_n = 2^n - 1$ is $(0, 0)$. Solving for $y = 0$ gives $0 = x^3 - 12x = x(x^2 - 12)$, so $x = 0$ or $x^2 = 12$. However, 12 is not a square mod M_n by Case 2 of chapter 2, so the only relevant solution is $x = 0$, which leads to the point $(0, 0)$.

Remark 4.4 The only point of order 2 on the elliptic curve $y^2 = x^3 - 7^3$ over $\mathbb{F}_{H_n}$ with $H_n = 3 \cdot 8^n - 1$ or $H_n = 12 \cdot 8^n - 1$ is $(7, 0)$. $y = 0$ implies $x^3 = 7^3$ and since $x \mapsto x^3$ is a bijective map from $\mathbb{F}_{H_n}$ to itself, there is only one solution: $x = 7$, which leads to the point $(7, 0)$.

Remark 4.5 Suppose P is not divisible by 2 over the elliptic curve $y^2 = x^3 - 7^3$ over $\mathbb{F}_{H_n}$ with $H_n = 3 \cdot 2^n - 1$ and H_n prime. The order of P is either 2^n or $3 \cdot 2^n$, since P is not divisible by 2. If the order of P is 2^n then the order of $3P$ is also 2^n since $3 \not| 2^n$. If the order of P is $3 \cdot 2^n$, then the order of $3P$ is 2^n, since $\frac{3 \cdot 2^n}{3} = 2^n$. Hence the order of $3P$ is 2^n.

5 B. H. Gross Mersenne prime test

As mentioned at the end of chapter 3, B. H. Gross developed another test for Mersenne numbers. This test (and Gross' article [5]) is the basis for this paper. While it tests exactly the same as the Lucas-Lehmer test, it is less convenient in its calculations, but it gives rise to a more general idea of checking whether a number is prime, as will be shown in the next chapter as well as in the discussion. With the knowledge about elliptic curves from the previous chapter, we can immediately state and prove Gross' elliptic curve test for Mersenne numbers.

Gross' test for Mersenne numbers

Given an odd number $n > 3$ and corresponding Mersenne prime $M_n = 2^n - 1$, M_n is prime if and only if $x_k(x_k^2 - 12)$ is relatively prime to M_n for $0 \leq k \leq n-2$ and $gcd(x_{n-1}, M_n) > 1$, where $x_0 = -2$ and $x_k = \frac{(x_{k-1}^2 + 12)^2}{4x_{k-1}(x_{k-1}^2 - 12)}$.

Proof of sufficiency of Gross' test

Suppose $x_k(x_k^2 - 12)$ is relatively prime to M_n for $0 \leq k \leq n-2$ and $gcd(x_{n-1}, M_n) > 1$. Also assume M_n is composite. Since $M_n = 3 \bmod 4$, there is at least one divisor of M_n which is 3 mod 4 as well. Take such a divisor $q \leq \frac{1}{5} M_n$, which exist since if $M_n = q \cdot r$ with $q \equiv 3 \bmod 4$, then $r \equiv 1 \bmod 4$ and thus $r \geq 5$. Then according to Lemma 4.2 the number of points on the elliptic curve mod q is $q + 1$. So the order of the point $P = (-2, 4)$ on $y^2 = x^3 - 12x \bmod q$ divides $q + 1$. However, since $x_k(x_k^2 - 12)$ are relatively prime to M_n for $0 \leq k \leq n - 2$, they are also relatively prime to q for the same k. So the order must be 2^n as well. However $q + 1 < \frac{M_n}{4} < 2^n$. This is the required contradiction, so M_n is not composite and therefore prime. ■

Proof of necessity of Gross' test

Suppose M_n is prime, then according to Lemma 4.2 the number of points on the elliptic curve is $M_n + 1 = 2^n$, since $2^n - 1 \equiv 3 \bmod 4$ for $n \geq 2$. The point P with $x = x_0 = -2$ is not divisible by 2 according to Remark 4.1 and the order of P divides the number of elements 2^n. Hence the order of $P = 2^n$, which means $(2^{(n-1)})P$ has order 2 and thus by Lemma 4.3 $(2^{(n-1)})P \equiv (0, 0)$ mod M_n. Therefore $(2^k)P$ is relatively prime to M_n for $0 \leq k \leq p - 2$ and $gcd(x_{n-1}, M_n) > 1$. ■

Since the Lucas-Lehmer test is so efficient in its calculations, Gross' test is interesting for the theory and the mechanics, but has no real use in practice. However, during the research of this paper, a similar test to Gross' test has been derived which in principle is the same, but tests a different group of numbers.

6 Another Elliptic Curve variant

The prime test in the previous chapter leads to the idea of similar tests using different elliptic curves and different starting points. In this chapter, a test will be proven for numbers of the shape $H_n = 3 \cdot 8^n - 1$ and $H_n = 12 \cdot 8^n - 1$. The elliptic curve used for both cases is $y^2 = x^3 - 7^3$. Using Lemmas from the section Elliptic Curves and a similar idea to Gross' test, we can now construct the following tests:

Theorem 1

A number $H_n = 3 \cdot 8^n - 1$, $n > 0$ is prime if and only if x_k is well-defined mod H_n for $0 \leq k \leq 3n - 1$, i.e. $(x_k^3 - 7^3)$ is a unity mod H_n for $0 \leq k \leq 3n - 2$ and $x_{3n-1} \equiv 7 \bmod H_n$, where $x_0 = \frac{763}{9}$ and $x_{k+1} = \frac{x_k^4 + 8 \cdot 7^3 x_k}{4 \cdot (x_k^3 - 7^3)}$.

Proof of sufficiency of Theorem 1

Given x_i well-defined mod H_n for $i \leq 3n - 1$ and $x_{3n-1} = 7$, assume H_n is composite. Since H_n is 2 mod 3 it has a divisor 2 mod 3. Take such a divisor q for which $q \leq \frac{1}{7} M_n$, which exist since if $H_n = q \cdot r$ with $q \equiv 2 \bmod 3$, then $r \equiv 1 \bmod 3$ and thus $r \geq 7$, since $r = 4$ would lead to H_n even. Then the elliptic curve $y^2 = x^3 - 7^3$ mod q has $q + 1$ points by Lemma 4.3, so the order of an element must divide $q + 1$. Since q divides H_n, x_i for $i \leq 3n - 1$ is well-defined mod q and $x_{3n-1} \equiv 7 \bmod q$. Therefore the order of the point Q with x-coordinate $\frac{763}{9}$ is 2^{3n} and thus the order of $P = (14, 49)$ for which $3P = Q$ is $3 \cdot 2^{3n} = 3 \cdot 8^n$. However, $q + 1$ is less then $\frac{1}{6} H_n < H_n < 3 \cdot 8^n$. This is a contradiction and therefore H_n is not composite, but prime. ■

Proof of necessity of Theorem 1 Given $H_n = 3 \cdot 8^n - 1$ prime. According to Remark 4.2, the point $P = (14, 49)$ is not divisible by 2, so the order of $3P$ is 2^{3n} by Remark 4.5. This implies that $(2^{3n-1} \cdot 3)P$ has order 2, so $(2^{3n-1} \cdot 3)P = (7, 0)$ by Remark 4.4. Hence $x_{3n-1} = 7$ and x_i for $i \leq 3n - 1$ is well-defined mod H_n. ■

Theorem X A number $H_n = 12 \cdot 8^n - 1$ is prime if and only if x_i is well-defined mod H_n for $i \leq 3n + 1$ and $x_{3n+1} \equiv 7 \bmod H_n$, where $x_0 = \frac{763}{9}$ and $x_{k+1} = \frac{x_k^4 + 8 \cdot 7^3 x_k}{4 \cdot (x_k^3 - 7^3)}$.

Proof of Theorem 2

$H_n = 12 \cdot 8^n - 1 \equiv 2 \bmod 3$ and $12 \cdot 8^n - 1 \equiv 3 \bmod 4$, so the proof is almost equivalent to the proof of Theorem 1. The same Lemmas and remarks apply, the only difference is the amount of steps necessary, which is 2 more to make 12 instead of 3. ■

These test open up possibilities to check a whole new group of numbers, namely the subgroup of $H_n = 3 \cdot 2^n - 1$ where $n \not\equiv 1 \bmod 3$. For the $n \equiv 1 \bmod 3$, Remark 4.2 does not hold unfortunately. What remains is to use the test to actually crunch some numbers and to discuss and conclude this paper.

7 Results, conclusion and discussion

7.1 Results

Using the tests from chapter 6, it is possible to test numbers of the form $3 \cdot 8^n - 1$ as well as the form $12 \cdot 8^n - 1$. Without further optimising the program by taking out n for which the numbers are certainly composite, the following numbers are prime in the range of exponents $[1, 20000)$ for $3 \cdot 8^n - 1$:

exponent	number
1	$3 \cdot 8^1 - 1$
2	$3 \cdot 8^2 - 1$
6	$3 \cdot 8^6 - 1$
72	$3 \cdot 8^{72} - 1$
102	$3 \cdot 8^{102} - 1$
108	$3 \cdot 8^{108} - 1$
1092	$3 \cdot 8^{1092} - 1$
4966	$3 \cdot 8^{4966} - 1$
6041	$3 \cdot 8^{6041} - 1$
6273	$3 \cdot 8^{6273} - 1$
13876	$3 \cdot 8^{13876} - 1$
17129	$3 \cdot 8^{17129} - 1$

and in the range of exponents $[1, 10000)$ for $12 \cdot 8^n - 1$:

exponent	number
3	$12 \cdot 8^3 - 1$
12	$12 \cdot 8^{12} - 1$
47	$12 \cdot 8^{47} - 1$
68	$12 \cdot 8^{68} - 1$
152	$12 \cdot 8^{152} - 1$
156	$12 \cdot 8^{156} - 1$
275	$12 \cdot 8^{275} - 1$
424	$12 \cdot 8^{424} - 1$
2519	$12 \cdot 8^{2519} - 1$
8819	$12 \cdot 8^{8819} - 1$

The implementation of the test was not the primary focus of the paper, so there is a lot of room left for improvement.

7.2 Conclusion and discussion

Using Gross' test as a basis, it was possible to construct two new tests. The way these tests work results in the idea that it might be applicable to an even wider range of numbers as well as elliptic curves. However, it is not easy to find suitable elliptic curves for which the necessary properties are guarantueed. A more general test might therefore be difficult or even impossible to obtain. This does not mean that these three tests are the only possible tests though and for further research finding more tests similar to the ones in this paper is definitely an option. As for the tests themselves, for the use in this paper they are implemented in the most basic way, so there is most likely a lot of optimization to be done. As with the Mersenne numbers, at the time of publishing this paper, it is unknown whether the primes of the form $3 \cdot 8^n - 1$ and $12 \cdot 8^n - 1$ are infinite or not, but searching for them could be interesting. Since both forms are of the shape $3 \cdot 2^n - 1$ it might even be useful in some very specific cases of twin primes, but that is probably the least relevant application.

References

[1] proofwiki, Euler's Criterion, https://www.proofwiki.org/wiki/Euler%27s_Criterion

[2] wikipedia, Proofs of quadratic reciprocity, http://en.wikipedia.org/wiki/Proofs_of_quadratic_reciprocity

[3] wikipedia, Lucas-Lehmer primality test, http://en.wikipedia.org/wiki/Lucas%E2%80%93Lehmer_primality_test

[4] A proof of the Lucas-Lehmer test, http://primes.utm.edu/notes/proofs/LucasLehmer.html

[5] B. H. Gross, *An elliptic curve test for Mersenne primes*, Journal of Number Theory 110, Januari 2005, http://www.sciencedirect.com/science/journal/0022314X/110/1

[6] Explicit Addition Formulae, http://crypto.stanford.edu/pbc/notes/elliptic/explicit.html

[7] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, 1984 by Springer-Verlag New York Inc., ISBN: 0-387-96029-5 and 3-540-96029-5.

[8] A. Silverberg, *Group Order Formulas for Reductions of CM Elliptic Curves*, http://www.math.uci.edu/~asilverb/bibliography/silverbergagct.pdf

[9] Erika Bakker, *Congruente getallen en concurrente lijnen*, april 2012, Masterthesis Rijksuniversiteit Groningen