MERSENNE NUMBERS

Conjecture 1

There exist no such element from M_p ***with an order***
that is a multiple of p^2 ***.***

Let $\mathbf{M_p = 2^p - 1}$ *be an Mersenne number , and* $\mathbf{a}$ *an element from* M_p.
$a^{p*p} \equiv 1\ (mod\ M_p) \implies a^p \equiv 1\ (mod\ M_p)$

equivalent is this:
Let $order(x)$ *be the order of* x.
$order(x) \not\equiv\ 0\ (mod\ p^2)$

Proposition 1

If M_p ***is not prime, when this is true:*** $\varphi(\mathbf{M_p}) \equiv \mathbf{0}\,(\mathbf{mod}\,\mathbf{p^2})$

It is well known that every primedivisor from M_p *has the following form:* $(2*k*p+1)$.

Let $M_p = 2^p - 1 = u * v = (2 * k_1 * p + 1) * (2 * k_2 * p + 1)$ *, with* u, v *are primes.*

When it is $\varphi(M_p) = (u-1) * (v-1) = (2 * k_1 * p) * (2 * k_2 * p)$.

It is now easy to see that p^2 *is an divisor of* $\varphi(M_p)$.

Therefore it is true that for every nonprime Mersenne-number this is valid : $\varphi(M_p) \equiv 0\,(mod\,p^2)$.

Proposition 2

If $\mathbf{M_p}$ ***is prime and the Conjecture 1 is correct,***
then all elements with the order $\mathbf{p}$
have the form $\mathbf{2^x}$ ***, with*** $\mathbf{x \in \{1, 2, 3, 4, .., p-1\}}$

PROOF:
Let M_p *be prime, then it is* $\varphi(M_p) = 2^p - 2 = p * k$ *with* $k \not\equiv 0 \,(mod\, p)$
Therefore the order p *occurs exactly* $\varphi(p) = (p-1)$ *.*
(Because M_p *is a cyclic group)*
$2^p - 1 \equiv 0 \Longrightarrow 2^p \equiv 1$
raised to the x*-th power:*
$((2^p)^x \equiv 1^x \equiv 2^{p*x} \equiv (2^x)^p \equiv 1$

Proposition 3

$\mathbf{a^k \equiv 2^x}$ ***with*** $\mathbf{a, k, x \in N}$ ***only possible, if*** $\mathbf{order(a) \equiv 0 \,(mod\, p)}$***.***

PROOF:
This is easy to show:
If a *creates* 2^x *then* a *creates all* $(2^x)^z$ *with* $z \in \mathbf{N}$
And because $(2^x)^p \equiv 1$ *is true, it must be* $order(a) \equiv 0 \,(mod\, p)$ *.*

Proposition 4

Let $\mathbf{M_p}$ ***be prime and let Conjecture 1 be correct.***
If $\mathbf{a}$ ***is an element of*** $\mathbf{M_p}$ ***with the order*** $\mathbf{p*k}$**,**
then this is true : $\mathbf{a^{\frac{\varphi(M_p)}{p}} \equiv 2^x}$ ***with*** $\mathbf{0 < x < p}$**.**

PROOF:

$a^{p*k} \equiv 1$

$k \not\equiv 0 \,(mod\, p)$ *is true because Conjecture 1.*

So, now taking the $p-th$ *root:* $a^k \equiv \sqrt[p]{1}$.

Because 2^x *are the only ones with the order* p

when M_p *is prime (because Conjecture 1), therefore this is true:* $a^k \equiv \sqrt[p]{1} \equiv 2^x$

Because $a^k \not\equiv 1$ *is true, this must also be true:* $2^x \not\equiv 1$.

If $order(a) = p*k$ *and* $a^{\frac{p*k}{p}} \equiv 2^x \not\equiv 1$,
then also $a^{\frac{\varphi(M_p)}{p}} \equiv 2^y \not\equiv 1$ *with* $y \in \mathbf{N}$

Because $(p*k)*z = \varphi(M_p)$, *with a* $z \in \mathbf{N}$
$a^{\frac{p*k}{p}} \equiv 2^x \Rightarrow (a^{\frac{p*k}{p}})^z \equiv a^{\frac{p*k*z}{p}} \equiv a^{\frac{\varphi(M_p)}{p}} \equiv (2^x)^z \equiv 2^{(x*z)}$

And therefore it must be :

Let M_p *be prime and* $order(a) = p*k$ *when it is:*
$a^{\frac{\varphi(M_p)}{p}} \equiv 2^x$ *with* $0 < x < p$.

Proposition 5

Let $\mathbf{M_p}$ ***be non-prime and Conjecture 1 is correct.***
If $\mathbf{a}$ ***is an element from*** $\mathbf{M_p}$ ***with the order*** $\mathbf{p*k}$
when it must be : $\mathbf{a}^{\frac{\varphi(\mathbf{M_p})}{\mathbf{p}}} \equiv \mathbf{1}$.

PROOF:

In general is: $a^{\varphi(M_p)} \equiv 1$ *and* $p*k$ *must be a divisor of* $\varphi(M_p)$.

Let $\varphi(M_p) = p*k*z$, *with an* $z \in \mathbf{N}$

That $k \not\equiv 0\ (mod\, p)$ *is true , can be seen in the Conjecture 1.*

Therefore it is: $z \equiv 0\ (mod\, p)$, *because* $\varphi(M_p) \equiv 0\ (mod\, p^2)$

$a^{p*k} \equiv 1 \ \Rightarrow\ (a^{(p*k)})^z \equiv 1^z \equiv a^{p*k*z}$

Let $z = p*m$ *with an* $m \in \mathbf{N}$ *then it is:* $a^{p*k*p*m} \equiv 1$

Now taking the $p-th$ *root:*

$a^{\frac{p*k*p*m}{p}} \equiv a^{p*k*m} \equiv (a^{p*k})^m \equiv 1^m \equiv 1 \equiv a^{\frac{\varphi(M_p)}{p}}$

Proposition 6

Let M_p ***be an Mersenne Number, then it is:***

$\mathbf{ord(3) \equiv 0 \,(mod\, p)} \;\vee\; \mathbf{ord(6) \equiv 0 \,(mod\, p)}$

PROOF:

CASES:

I.) If $ord(3) \equiv 0 \,(mod\, p)$ *is true, then the Proposition 6 is correct.*

II.) If $ord(3) \not\equiv 0 \,(mod\, p)$*:*

Because $ord(2) = p$ *is always true , then this is correct:*

$gcd(ord(2), ord(3)) = 1$

(gcd is the greatest common divisor-funktion)

And therefore:

$ord(6) = ord(2 * 3) = ord(2) * ord(3) = p * ord(3)$

$\Rightarrow ord(6) \equiv 0 \,(mod\, p)$

Conclusion:
I had til now no success to proof that the Conjecture 1 is correct.
My main intention in this pdf was to show, that :
If $M_p = 2^p - 1$ is prime, when there exists an x with $0 < x < p$, so that

$$3^{\frac{(2^p-2)}{p}} \equiv 2^x \, (mod \, 2^p - 1)$$

is true.
And if $M_p = 2^p - 1$ is not prime then where exist none such x.
That means that the element 3 plays a special role here,
and this test would be an non-probabilistic test
But i had no success to show that.
I think that Catalan's conjecture could be the reason why the number 3 plays
here such an special role. (http://en.wikipedia.org/wiki/Catalan%27s_conjecture)

I know when this Mersenne-test would be an non-probabilistic-test, the complexity of time would be the same
as the Lucas-Lehmer test when it is implemented in the naive way.
But it could be that someone could make this faster than the Lucas-Lehmer test.

One interesting observation is this:

When M_p is prime then it is possible to find an k for every x so that

$2^x \equiv 3^k \, (mod \; 2^p - 1)$

And therefore:
$2^p - 1 \equiv 2^0 + 2^1 + 2^2 + 2^3 + ... + 2^{p-1} \equiv 3^{\frac{1*w}{p}} + 3^{\frac{2*w}{p}} + 3^{\frac{3*w}{p}} + ... + 3^{\frac{p*w}{p}}$
with $w = (2^p - 2)$

Also interesting is:

Because every 2^x can be expressed with an k , so that $3^k \equiv 2^x$ is true when $2^p - 1$ is prime.
The following is correct:
There exist an $t \in \mathbf{N}$ and an k, so that: $3^k - 2^2 = (2^p - 1) * t$ is true.
(This is an equation, not an congruent-sign !)
Equivalent is this:
$k = log_{(3)}((2^p - 1) * t - 4)$

this means if there exist an $t \in \mathbf{N}$ and an $k \in \mathbf{N}$ so that the equation ist true,
when $2^p - 1$ is prime !

This document was written by Sascha Pfaller

When you found some mistakes or if you have some questions
do not hesitate to contact me:
Email:Sascha-Pfaller@web.de
(If possible please mention the word 'mersenne' in the subject so I know that the email is no Spam. ;-)