Seien $m \neq n$ und a von Null verschiedene natürliche Zahlen. Es ist zu beweisen, dass

$ggT(a^{(2^m)}+1, a^{(2^n)}+1)=1$, falls a eine gerade Zahl ist,

und $ggT(a^{(2^m)}+1, a^{(2^n)}+1)=2$, falls a eine ungerade Zahl ist.

Lösung:

Die 3. binomische Formel heißt: $(x+y)\cdot(x-y)=(x-y)\cdot(x+y)=x^2-y^2$.

Weil $m \neq n$ definiert wurde, kann man ohne Einschränkung $m > n$ setzen, d.h. es existiert ein $k \in \mathbb{N}$ mit $m = n+k$.

Aus $ggT(a^{(2^m)}+1, a^{(2^n)}+1)$ wird dadurch $ggT(a^{(2^{n+k})}+1, a^{(2^n)}+1)$.

Man muss jetzt zeigen, dass $(a^{(2^n)}+1) \mid (a^{(2^m)}+1)$ gilt, also dass die Zahl $(a^{(2^n)}+1)$ die Zahl $(a^{(2^m)}+1)=(a^{(2^{n+k})}+1)$ teilt.

Das erreicht man durch <u>mehrmalige Anwendung der o.g. binomischen Formel</u>:

Zunächst erhält man für $x=a^{(2^n)}, y=1$:

$$(a^{(2^n)}+1)\cdot(a^{(2^n)}-1)=(a^{2^n})^2-1^2=a^{2^n}\cdot a^{2^n}-1=a^{2^n+2^n}-1=a^{2\cdot 2^n}-1=a^{2^{n+1}}-1$$

Anschließend erhält man für $x=a^{(2^{n+1})}, y=1$:

$$(a^{(2^{n+1})}-1)\cdot(a^{(2^{n+1})}+1)=(a^{2^{n+1}})^2-1^2=a^{2^{n+1}}\cdot a^{2^{n+1}}-1=a^{2^{n+1}+2^{n+1}}-1=a^{2\cdot 2^{n+1}}-1=a^{2^{n+2}}-1$$

Zusammengefasst hat man also bis jetzt

$(a^{(2^n)}+1)\cdot(a^{(2^n)}-1)\cdot(a^{(2^{n+1})}+1)=a^{2^{n+2}}-1$ und das bedeutet, dass $(a^{(2^n)}+1) \mid (a^{(2^{n+2})}-1)$

Dieses Verfahren wird nun solange fortgesetzt, bis man nach dem Gleichheitszeichen $(a^{(2^m)}-1)$ erhält, was ja mit $(a^{(2^{n+k})}-1)$ identisch ist.

Im letzten Schritt erhält man für $x=a^{(2^{n+k-1})}, y=1$

$$(a^{(2^{n+k-1})}-1)\cdot(a^{(2^{n+k-1})}+1)=(a^{2^{n+k-1}})^2-1^2=a^{2^{n+k-1}}\cdot a^{2^{n+k-1}}-1=a^{2^{n+k-1}+2^{n+k-1}}-1=a^{2\cdot 2^{n+k-1}}-1$$

$$=a^{2^{n+k-1+1}}-1=a^{2^{n+k}}-1$$

Der gesamte Ausdruck heißt also:

$(a^{(2^n)}+1)\cdot(a^{(2^n)}-1)\cdot(a^{(2^{n+1})}+1)\cdot(a^{(2^{n+2})}+1)\cdot\ldots\cdot(a^{(2^{n+k-1})}+1)=a^{2^{n+k}}-1=a^{2^m}-1$ und

das bedeutet, dass $(a^{(2^n)}+1) \mid (a^{(2^{n+k})}-1) \Leftrightarrow (a^{(2^n)}+1) \mid (a^{(2^m)}-1)$.

Es existiert also ein d mit

$$(a^{(2^n)}+1)\cdot d=(a^{(2^m)}-1) \Leftrightarrow (a^{(2^n)}+1)\cdot d+2=(a^{(2^m)}-1)+2$$

$$\Leftrightarrow (a^{(2^n)}+1)\cdot d+2=a^{(2^m)}-1+2=(a^{(2^m)}+1)$$

Es gelten folgende Teilbarkeitsregeln:

$v=q\cdot w+r \Leftrightarrow r=v-q\cdot w$

Setzt man $ggT(v,w)=e$, dann gelten auch folgende Aussagen:

$e|v \wedge e|w \Rightarrow e|v-w$

$e|w \Rightarrow e|q \cdot w$. Aus beiden Aussagen ergibt sich auch $e|v \wedge e|q \cdot w \Rightarrow e|v-q \cdot w$

Da nun $r=v-q \cdot w$ ist, folgt aus $e|v-q \cdot w \Rightarrow e|r$

Also lässt sich folgern:

Wenn $ggT(v,w)=e$ und $e|w \wedge e|r$, dann gilt auch $ggT(w,r)=e$

Man definiert $v=(a^{(2^m)}+1), w=(a^{(2^n)}+1), d=e, r=2$

Es gilt also nach $ggT(v,w)=ggT(w,r)$

$ggT(a^{(2^m)}+1, a^{(2^n)}+1)=ggT(a^{(2^n)}+1,2)$

Ist a eine gerade Zahl, dann ist $a^{(2^n)}+1$ eine ungerade Zahl,

d.h. $ggT(a^{(2^n)}+1,2)=1=ggT(a^{(2^m)}+1, a^{(2^n)}+1)$

Ist a eine ungerade Zahl, dann ist $a^{(2^n)}+1$ eine gerade Zahl,

d.h. $ggT(a^{(2^n)}+1,2)=2=ggT(a^{(2^m)}+1, a^{(2^n)}+1)$.

Was zu beweisen war.