ÜBER DIE AUFLÖSUNG DER GLEICHUNG:

$\varphi(x)=n,$

wenn $\varphi(m)$ die Anzahl derjenigen Zahlen bezeichnet, welche relativ prim zu m und kleiner als m sind.

(Von Prof. **Alois Pichler.**)

Die Anzahl derjenigen Zahlen, welche kleiner als eine gegebene Zahl m und relativ prim zu m sind, ist offenbar nur von m abhängig und durch m selbst vollständig bestimmt; somit ist diese Anzahl eine Function von m und wird nach *Gauss* mit $\varphi(m)$ bezeichnet. Der Wert der Function $\varphi(m)$ lässt sich leicht berechnen, wenn die Zusammensetzung der Zahl m aus Primfactoren bekannt ist. Wenn nämlich:

$$m=p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}\ \ldots\ p_k^{\alpha_k},$$

so ist:

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Nehmen wir nun aber an, es sei uns $\varphi(m)$ gegeben und wir hätten daraus den Wert des Argumentes m zu bestimmen, d. h. die Gleichung:

$$\varphi(x)=n, \qquad \ldots\ldots\ldots \quad 1)$$

worin n eine gegebene Zahl bedeutet, aufzulösen. Dass diese Gleichung nicht für jeden beliebigen, ganzzahligen Wert von n Lösungen besitzen wird, erhellt schon daraus, dass $\varphi(m)$ immer eine gerade Zahl ist, ausgenommen die beiden Fälle $m=1$ und $m=2$, für welche der Wert der Function gleich der Einheit ist.

Es hat daher die Geichung:

$$\varphi(x)=1$$

die beiden Lösungen: $x=1$ und $x=2$.

Für jedes andere ungerade n ist dagegen die Gleichung 1) unmöglich.

Schliessen wir diesen einzigen Fall, in welchem n eine ungerade Zahl ist, aus, so muss, damit die Gleichung 1) überhaupt Lösungen besitzt, n eine gerade Zahl sein. Weil ferner:

$$\varphi\,[2\,(2m+1)]=\varphi\,(2m+1)$$

ist, so erhalten wir aus jeder ungeraden Lösung der Gleichung 1) durch Verdopplung sogleich eine zweite Lösung. Weiters können wir schon von vornherein sagen, dass hauptsächlich die Häufigkeit des Primfactors 2 in der gegebenen Zahl n für die Anzahl der Lösungen der Gl. 1) ausschlaggebend sein wird.

I.) Betrachten wir zuerst den Fall, dass die gegebene Zahl eine Potenz von 2 ist, also die Gleichung:

$$\varphi(x) = 2^n \quad . \; . \; . \; . \; . \; . \; . \; . \quad 2)$$

vorliegt. Die allgemeinste Darstellung der Zahl x ist gegeben durch

$$x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \; . \; . \; . \; ;$$

daher: $\varphi(x) = p_1^{\alpha_1 - 1} \, p_2^{\alpha_2 - 1} \; . \; . \; . \; . \; (p_1 - 1)(p_2 - 1) \; . \; . \; . \; . = 2^n.$

Da auf der rechten Seite des Gleichheitszeichens nur der Primfactor 2 vorkommt, so darf auch links kein anderer Primfactor erscheinen; mithin muss:

$$p_1 = 2 \text{ und } \alpha_2 - 1 = \alpha_3 - 1 = \; . \; . \; . \; . = 0,$$

also: $\alpha_2 = \alpha_3 = \; . \; . \; . \; . \; = 1$ sein.

Die gesuchte Zahl x muss daher die folgende Form haben:

$$x = 2^\alpha p_2 \, p_3 \; . \; . \; . \; . \; . \; . \; ,$$

d. h. die ungeraden Primfactoren dürfen nur in der ersten Potenz vorkommen.

Die Gleichung für $\varphi(x)$ nimmt nun folgende einfachere Gestalt an:

$$\varphi(x) = 2^{\alpha - 1}(p_2 - 1)(p_3 - 1) \; . \; . \; . \; . \quad = 2^n \; . \; . \; . \; . \quad 3)$$

Diese Gleichung ist erfüllt, wenn außer 2 kein anderer Primfactor in der Zahl x vorkommt, mit anderen Worten, wenn x selbst auch eine Potenz von 2 ist. Setzen wir also:

$$x = 2^\alpha,$$

so muss: $2^{\alpha - 1} = 2^n$, mithin $\alpha = n + 1$ sein.

Als erste Auflösung der Gl. 2) erhalten wir demnach:

$$x = 2^{n+1}$$

Die Gl. 3) wird aber auch durch folgende Annahme befriedigt:

$$p_2 - 1 = 2^\beta, \quad p_3 - 1 = 2^\gamma \; . \; . \; . \; . \; . \; ,$$

woraus: $p_2 = 2^\beta + 1, \; p_3 = 2^\gamma + 1 \; . \; . \; . \; . \; .$ folgt.

Alle diese Zahlen haben die Form $2^k + 1$ und müssen Primzahlen sein. Damit aber eine Zahl von dieser Form eine Primzahl sein kann, muss der Exponent k selbst eine Potenz von 2 sein. Infolge dessen schreiben wir gleich:

$$p_2 = 2^{2^\beta} + 1, \quad p_3 = 2^{2^\gamma} + 1 \; . \; . \; . \; .$$

Die Zahl x kann daher auch die Form haben:

$$x = 2^\alpha \, (2^{2^\beta} + 1)\,(2^{2^\gamma} + 1) \; . \; . \; . \; . \; ,$$

worin α auch den Wert 0 haben kann. Dann ist:

$$\varphi(x) = 2^{\alpha - 1} \cdot 2^{2^\beta} \cdot 2^{2^\gamma} \; . \; . \; . = 2^n.$$

Da in dieser Lösungsform auch die oben erhaltene erste Auflösung als specieller Fall enthalten ist, nämlich für $\alpha = n + 1$, so können wir sagen:

Die Gleichung: $\varphi(x) = 2^n$

ist immer möglich; ihre Lösungen haben die Form:

$$x = 2^\alpha \left(2^{2^\beta} + 1\right)\left(2^{2^\gamma} + 1\right)\ldots,$$

worin: $\alpha = 0, 1, 2, \ldots \; n + 1$ sein kann.

Für $\alpha = 0$, muss: $2^\beta + 2^\gamma + \ldots = n$,

" $\alpha > 0$, " $(\alpha - 1) + 2^\beta + 2^\gamma + \ldots = n$ sein.

Außerdem dürfen von den Exponenten $\beta, \gamma \ldots$ nicht zwei einander gleich sein, weil jeder ungerade Primfactor nur in der ersten Potenz vorkommen darf.

Da eine Zahl von der Form $2^{2^\nu} + 1$ für $\nu = 0$ bis einschließlich $\nu = 4$ eine Primzahl ist, so können wir mittelst dieser Primzahlen alle Potenzen von 2 bis einschließlich 2^{31} ausdrücken und daher auch die Anzahl der Lösungen bis zu dieser Grenze angeben. Weil nämlich eine gegebene Zahl n nur auf eine einzige, ganz bestimmte Weise als Summe verschiedener Potenzen der Zahl 2 dargestellt werden kann, so liefert jeder Wert von α nur eine Auflösung. Somit erhalten wir so viele Auflösungen, als es verschiedene Werte von α gibt, nämlich $n + 2$. Daher folgt der Satz:

Die Gleichung: $\varphi(x) = 2^n$ hat für $n > 32$ $n + 2$ Lösungen.

In diesem Satze ist auch der frühere Ausnahmsfall $n = 0$ mitinbegriffen. Unter diesen $n + 2$ Auflösungen befindet sich nur eine einzige ungerade Zahl, nämlich die für $\alpha = 0$ dargestellte, welche zugleich die kleinste aller Auflösungen ist; alle übrigen $n + 1$ Lösungen sind gerade Zahlen.

Für $n \overline{>} 32$ kann α nicht mehr alle Werte von 0 bis $n + 1$ durchlaufen, weil sowohl $2^{32} + 1$ als auch $2^{64} + 1$ keine Primzahl ist. Erstere ist durch 641 theilbar, wie schon *Euler* nachgewiesen hat, und letztere durch 274177 theilbar, wie zuerst *Landry* gezeigt hat.

Es lässt sich nun leicht zeigen, dass für $n = 32 \ldots$ bis einschließlich $n = 127$ die Zahl der Lösungen constant, nämlich gleich 32 ist.

Es sei also: $\varphi(x) = 2^{32+\nu}$, worin $\nu = 0, 1, 2 \ldots 95$ sein kann.

Die Bedingungsgleichung lautet jetzt:

$$(\alpha - 1) + 2^\beta + 2^\gamma + 2^\delta + \ldots = 32 + \nu.$$

Um den kleinsten Wert für α zu erhalten, setzen wir für β, γ, δ die größtmöglichen Werte ein, nämlich:

$$(\alpha - 1) + 2^4 + 2^3 + 2^2 + 2 + 1 = 32 + \nu,$$

daher $\alpha + 30 = 32 + \nu$, folglich $\alpha = \nu + 2$.

$\nu + 2$ ist also der kleinste Wert für α, der größte ist aber $32 + \nu + 1$, somit die Anzahl der möglichen Werte von α und daher auch die Anzahl der Lösungen unserer Gleichung: $32 + \nu + 1 - (\nu + 1) = 32$.

Die Gleichung: $\varphi(x) = 2^{32+\nu}$ hat für $\nu = 0, 1, 2 \ldots 95$ immer 32 Lösungen, welche durchwegs gerade Zahlen sind.

Unter allen Gleichungen von der Form $\varphi(x) = 2^n$ hat von $n = 0$ bis $n = 127$ die Gleichung $\varphi(x) = 2^{31}$ die meisten Lösungen, nämlich 33.

Bemerkung. Kennt man die $n+2$ Auflösungen der Gleichung: $\varphi(x) = 2^n$, so braucht man, um die $n+3$ Lösungen der Gleichung: $\varphi(x) = 2^{n+1}$ zu erhalten, nur die durch $\alpha = 0$ dargestellte, ungerade Auflösung neu zu berechnen; die Verdopplung dieser, sowie der $n+1$ geradzahligen Auflösungen der ersten Gleichung ergeben die noch übrigen $n+2$ Auflösungen der zweiten Gleichung.

In der folgenden kleinen Tabelle sind die Auflösungen der Gleichung $\varphi(x) = 2^n$ für $n = 0$ bis $n = 10$ zusammengestellt.

$\varphi(n)$	n
1	1, 2.
2	3, 4, 6.
2^2	5, 8, 10, 12.
2^3	15, 16, 20, 24, 30.
2^4	17, 32, 34, 40, 48, 60.
2^5	51, 64, 68, 80, 96, 102, 120.
2^6	85, 128, 136, 160, 170, 192, 204, 240.
2^7	255, 256, 272, 320, 340, 384, 408, 480, 510.
2^8	257, 512, 514, 544, 640, 680, 768, 816, 960, 1020.
2^9	771, 1024, 1028, 1088, 1280, 1360, 1536, 1542, 1632, 1920, 2040.
2^{10}	1285, 2048, 2056, 2176, 2560, 2570, 2720, 3072, 3084, 3264, 3840, 4080.

Aus dieser Tabelle ist ersichtlich, dass manchmal der Wert der Function φ für zwei unmittelbar auf einander folgende Argumente derselbe ist: so z. B. für 1 und 2, 3 und 4, 15 und 16 u. s. w. Allgemein:

Lässt sich die Zahl $2^{2^n}-1$ in lauter Primfactoren von der Form $2^{2^\nu}+1$ zerlegen, so ist immer:

$$\varphi\left(2^{2^n}-1\right) = \varphi\left(2^{2^n}\right) = 2^{2^n}-1.$$

Es ist also für

$$\begin{array}{lll}
n = 0, & \varphi(1) & = \varphi(2) = 1 \\
n = 1, & \varphi(3) & = \varphi(4) = 2 \\
n = 2, & \varphi(15) & = \varphi(16) = 2^3 \\
n = 3, & \varphi(2^8-1) & = \varphi(2^8) = 2^7 \\
n = 4, & \varphi(2^{16}-1) & = \varphi(2^{16}) = 2^{15} \\
n = 5, & \varphi(2^{32}-1) & = \varphi(2^{32}) = 2^{31}.
\end{array}$$

Es ist z. B. im letzteren Falle:

$$2^{32}-1=(2^{16}+1)\ (2^8+1)\ (2^4+1)\ (2^2+1)\ (2+1),$$

somit $\varphi\ (2^{32}-1)=2^{16}\,.\,2^8\,.\,2^4\,.\,2^2\,.\,2=2^{31}=\varphi\ (2^{32})$.

Für $2^{64}-1$ trifft diese Eigenschaft nicht mehr zu, weil $2^{32}+1$ keine Primzahl ist.

II.) Wir nehmen nun an, n sei das Doppelte einer ungeraden Primzahl q, also $\varphi\ (x)=2q$.

Dann muss: $p_1^{\alpha_1-1}\,p_2^{\alpha_2-1}\ldots(p_1-1)\,(p_2-1)\ldots=2q\ldots\ldots 4)$ sein. Weil p_1-1 eine gerade Zahl sein muss, so setzen wir: $p_1-1=2q$, woraus $p_1=2q+1$ folgt.

Durch Einsetzung dieses Wertes in 4) erhalten wir:

$$(2q+1)^{\alpha_1-1}\,.\,p_2^{\alpha_2-1}\,(p_2-1)=1$$

Daher muss: $\alpha_1-1=0$, also $\alpha_1=1$ sein;

ferner: $p_2^{\alpha_2-1}\ldots(p_2-1)\ldots=1$ oder $\varphi\ (y)=1$,

woraus $y=1,\ 2$ folgt.

Wenn also $2q+1$ eine Primzahl ist, so erhalten wir die beiden Lösungen:

$$x_1=2q+1 \quad \text{und} \quad x_2=2\ (2q+1).$$

Außer diesen beiden Lösungen erhalten wir noch zwei andere, wenn speciell $q=3$ ist. Denn der Gl. 4) wird auch Genüge geleistet, wenn $p_1-1=2$, also $p_1=3$ ist.

Dann muss: $3^{\alpha_1-1}\,p_2^{\alpha_2-1}\,.\,(p_2-1)\ldots=q$ sein,

mithin: $q=3,\ \alpha_1-1=1$ oder $\alpha_1=2$

und wiederum: $p_2^{\alpha_2-1}\ldots(p_2-1)\ldots=\varphi\ (y)=1$.

In diesem Falle kommen also zu den beiden früheren Lösungen noch die zwei weiteren: $x_3=3^2$ und $x_4=2\,.\,3^2$ hinzu.

Die Gleichung: $\varphi\ (x)=6$

besitzt daher die folgenden vier Auflösungen:

$$x=7,\ 14,\ 9,\ 18.$$

Wenn wir den speciellen Fall: $q=3$, für welchen wir die vollständige Lösung soeben gefunden haben, ausschließen, so ergibt sich aus den voranstehenden Betrachtungen folgender Satz:

Die Gleichung: $\varphi\ (x)=2q$, worin q eine ungerade Primzahl >3 bedeutet, ist, wenn $2q+1$ eine Primzahl ist, immer möglich und hat die zwei Lösungen:

$$x_1=2q+1 \quad \text{und} \quad x_2=2\ (2q+1).$$

Ist hingegen $2q+1$ keine Primzahl, so ist die obige Gleichung unmöglich.

Alle Primzahlen, welche größer als 3 sind, haben die Form $6k\pm1$. Für $q=6k+1$ ist aber $2q+1=12k+3=3\ (4k+1)$, somit durch 3 theilbar. Daher ist die Gleichung:

$$\varphi\ (x)=2q \quad \text{für} \quad q=6k+1 \quad \text{immer unmöglich.}$$

Damit also die Gleichung überhaupt möglich ist, muss q von der Form $6k-1$ sein. Aber auch, wenn diese Bedingung erfüllt ist, wird die Gleichung nicht immer Lösungen besitzen, weil nicht immer $2q+1$ eine Primzahl sein wird. So ist z. B. $2q+1$ immer durch 5 theilbar, wenn $q=30k+17$ ist, und immer durch 7 theilbar, wenn $q=42k+17$ ist; hat ferner q die Form: $q=18k^2-1$,

so ist $$2q+1=36k^2-1=(6k+1)(6k-1),$$
also ebenfalls keine Primzahl.

Unter 100 gibt es folgende gerade Zahlen von der Form $2q$, für welche die Gleichung $\varphi(x)=2q$ unmöglich ist, nämlich:

$$2q=14,\ 26,\ 34,\ 38,\ 62,\ 74,\ 86,\ 94.$$

Durch Anwendung derselben Schlussfolgerungen wie oben gelangen wir zu folgendem, etwas allgemeineren Resultate:

Die Gleichung: $\varphi(x)=2q^n$, worin q eine ungerade Primzahl > 3 bedeutet, besitzt, wenn $2q^n+1$ eine Primzahl ist, immer die beiden Lösungen:

$$x_1=2q^n+1 \quad \text{und} \quad x_2=2\left(2q^n+1\right).$$

Ist aber $2q^n+1$ keine Primzahl, so ist die obige Gleichung unmöglich. Dagegen ist die specielle Gleichung: $\varphi(x)=2.3^n$ immer möglich und hat, wenn 2.3^n+1 eine Primzahl ist, die vier Lösungen:

$$x_1=2.3^n+1, \quad x_2=2\left(2.3^n+1\right); \quad x_3=3^{n+1}, \quad x_4=2.3^{n+1};$$

im entgegengesetzten Falle aber nur die letzteren zwei Lösungen.

So hat z. B. die Gleichung: $\varphi(x)=2.3^2=18$ die vier Lösungen: $x=19, 38, 27, 54$, während die Gleichung: $\varphi(x)=2.3^3=54$ nur zwei Lösungen besitzt, nämlich $x=81$, 162, weil 55 keine Primzahl ist.

Da für $q=6k+1$ auch q^n dieselbe Form hat, somit $2q^n+1$ wiederum durch 3 theilbar ist, so muss auch jetzt q abermals die Form $6k-1$ haben. Weil aber auch jede gerade Potenz von $6k-1$ die Form $6h+1$ hat, so folgt:

Die Gleichung: $\varphi(x)=2q^{2n}$ ist für $q>3$ immer unmöglich.

Die Gleichung: $\varphi(x)=2q^{2n+1}$ ist nur für $q=6k-1$ möglich.

III.) Es sei nun: $\varphi(x)=2^n q$ gegeben,

also: $$p_1^{\alpha_1-1} p_2^{\alpha_2-1} \ldots (p_1-1)(p_2-1)\ldots = 2^n q \ldots \quad 5)$$

a) Wir setzen nun: $p_1-1=2^{n-\nu}q$, worin $\nu=0, 1, 2 \ldots n-1$ sein kann; dann muss: $p_1=2^{n-\nu}q+1$ eine Primzahl sein.

Ist diese Bedingung erfüllt, so erhalten wir nach Einsetzung in 5)

$$\left(2^{n-\nu}q+1\right)^{\alpha_1-1} \cdot p_2^{\alpha_2-1}\,(p_2-1)\ldots = 2^{\nu}.$$

Da $2^{n-\nu}q+1$ relativ prim zu 2 ist, so muss $\alpha_1-1=0$, also $\alpha_1=1$ sein, wodurch Gl. 5) in

$$p_2^{\alpha_2-1}\ldots(p_2-1)\ldots=\varphi(y)=2^{\nu}\quad\ldots\quad 6)$$

übergeht.

Diese Gleichung ist nach I) immer lösbar und hat für $\nu<32$ $\nu+2$ Lösungen. Bezeichnen wir eine derselben mit a, so dass also $\varphi(a)=2^{\nu}$ ist, so ist:

$$x=a\,p_1=a\left(2^{n-\nu}q+1\right)$$

eine Lösung der vorgelegten Gleichung, wenn a relativ prim zu $2^{n-\nu}q+1$ ist. Diese Bedingung ist hier immer erfüllt, weil nach der Annahme q eine ungerade Primzahl ist, daher $2^{n-\nu}q+1$ niemals eine Primzahl von der Form $2^{2^k}+1$ sein kann. Demnach erhalten wir für ein bestimmtes ν, wenn wir a alle Wurzeln der Gl. 6) durchlaufen lassen, $\nu+2$ Lösungen der gestellten Aufgabe.

Wäre $2^{n-\nu}q+1$ für jeden Wert von $\nu=0, 1, 2 \ldots n-1$ eine Primzahl, so erhielten wir im ganzen: $2+3+4+\ldots n+1=\frac{n(n+3)}{2}$ Lösungen. Dies ist aber schon für $n>2$ bei $q=3$ nicht mehr der Fall und weiters kann eine Zahl von der Form 2^nq+1 für $q>3$ keine Primzahl sein, sondern ist durch 3 theilbar, wenn

$$n=2h \quad\text{und}\quad q=6k-1,$$

oder

$$n=2h+1 \quad \text{„} \quad q=6k+1 \quad \text{ist.}$$

Es kann daher eine Zahl von der obigen Form nur dann eine Primzahl sein, wenn

$$n=2h \quad\text{und}\quad q=6k+1,$$

oder

$$n=2h+1 \quad \text{„} \quad q=6k-1 \quad \text{ist.}$$

Es können also, wenn $q>3$ ist, höchstens für die Hälfte der obigen Werte von ν Primzahlen erscheinen. Sind nun $\nu_1, \nu_2, \nu_3 \ldots \nu_k$ diejenigen Werte von ν, für welche $2^{n-\nu}q+1$ Primzahlen sind so ist die Anzahl der Lösungen A gegeben durch:

$$A=\nu_1+\nu_2+\ldots\nu_k+2k.$$

b) Setzen wir aber:

$$p_1-1=2^{n-\nu} \quad\text{also}\quad p_1=2^{n-\nu}+1,$$

so muss:

$$n-\nu=2^{\lambda} \quad\text{und}\quad \lambda \overline{\gtrless} 4 \quad \text{sein.}$$

Setzen wir nun den Wert von $p_1=2^{2^\lambda}+1$ in die Gl. 5) ein, so geht sie über in:

$$\left(2^{2^\lambda}+1\right)^{\alpha_1-1} p_2^{\alpha_2-1}\,(p_2-1)\ldots=2^{\nu}q.$$

Diese Gleichung kann nur dann bestehen, wenn

$$q = 2^{2^\lambda} + 1 = p_1 \quad \text{und} \quad \alpha_1 = 2 \qquad \text{ist.}$$

Es bleibt dann noch die Gleichung aufzulösen:

$$p_2^{\alpha_2 - 1} \cdot \cdot (p_2 - 1) \ldots = \varphi(z) = 2^\nu = 2^n - 2^\lambda \ldots 7)$$

Damit diese Gleichung möglich ist, muss $2^\lambda \overline{\overline{<}} n$ sein.

Ist diese Bedingung erfüllt, so ist die Gl. 7) immer möglich und hat $n + 2 - 2^\lambda$ Lösungen. Bezeichnen wir eine dieser Lösungen mit b, so dass $\varphi(b) = 2^n - 2^\lambda$ ist, so ist

$$x = b\,q^2 = b\left(2^{2^\lambda} + 1\right)^2$$

eine Lösung der vorgelegten Gleichung, wenn b relativ prim zu q ist.

Wir erhalten somit aus 7) so viele Lösungen, als es Zahlen b gibt, die relativ prim zu q sind. Da nämlich nach I) alle Wurzeln b Primzahlen von derselben Form wie die von q enthalten, so kann in einem oder mehreren b die Primzahl q auftreten; somit werden im allgemeinen nicht mehr alle b zu q relativ prim sein.

Das Ergebnis unserer Betrachtungen können wir nun folgendermaßen zusammenfassen:

Die Gleichung: $\varphi(x) = 2^n q$

ist unmöglich, wenn keine der Zahlen $2^{n-\nu}q + 1$ für $\nu = 0, 1, 2 \ldots n - 1$ eine Primzahl ist und außerdem q keine Primzahl von der Form $2^{2^\lambda} + 1$ ist, oder wenn für ein solches q $2^\lambda > n$ ist.

Wenn aber wenigstens eine der oben angegebenen Zahlen eine Primzahl ist oder q die Form $2^{2^\lambda} + 1$ hat und $2^\lambda \overline{<} n$ ist, so hat die obige Gleichung immer Lösungen. Die Lösungen selbst haben die Form:

$\alpha)$ $x = a\left(2^{n-\nu}q + 1\right)$, worin a eine Lösung der Gl. $\varphi(y) = 2^\nu$ ist;

$\beta)$ $x = b\,q^2$, „ b „ „ „ „ $\varphi(z) = 2^{n-2^\lambda}$ „,

wobei b relativ prim zu q sein muss.

Unter 100 gibt es nur zwei Zahlen von der Form $2^n q$, für welche die Gl. III.) unmöglich ist, nämlich 76 und 68.

Die Gleichung: $\varphi(x) = 76 = 2^2.19$

ist unmöglich, weil weder $2^2.19 + 1 = 77$ noch $2\,19 + 1 = 39$ eine Primzahl ist. Aus demselben Grunde ist auch die Gleichung: $\varphi(x) = 68 = 2^2.17$ unmöglich, trotzdem 17 die Form $2^{2^2} + 1$ hat, da $2^2 > 2$ ist.

Um das angegebene Verfahren durch ein Beispiel zu erläutern, wollen wir folgende Gleichung auflösen:

$$\varphi(x) = 24 = 2^3\, 3.$$

Es muss nun $\qquad p = 2^{3-\nu}.3 + 1 \qquad$ sein.
Für $\nu = 1$ ist $p = 13$, für $\nu = 2$ ist $p = 7$.
Wir erhalten somit aus α) $1 + 2 + 2 . 2 = 7$ Lösungen.

Die Gleichung: $\varphi(y) = 2$ hat die Lösungen: $y = 3, 4, 6$,
somit ist: $\quad x_1 = 39, \quad x_2 = 52, \quad x_3 = 78.$

Die Gleichung: $\varphi(y) = 2^2$ hat die Lösungen: $y = 5, 8, 10, 12$,
also ist: $\quad x_4 = 35, \quad x_5 = 56, \quad x_6 = 70, \quad x_7 = 84.$

Dann hat aber auch 3 die Form $2^1 + 1$, somit ist $2^\lambda = 1$ und $1 < 3$.

Die Gleichung: $\varphi(z) = 2^{3-1} = 2^2$ hat die Lösungen: $z = 5, 8, 10, 12$.

Von diesen sind aber nur die ersten drei relativ prim zu 3; durch Multiplication dieser drei Zahlen mit $3^2 = 9$ erhalten wir noch weitere drei Lösungen, nämlich:

$$x_8 = 45, \quad x_9 = 72, \quad x_{10} = 90.$$

Die Gleichung: $\varphi(x) = 24$ hat somit 10 Lösungen, welche der Größe nach geordnet sind:

$$x = 35,\ 39,\ 45,\ 52,\ 56,\ 70,\ 72,\ 78,\ 84,\ 90.$$

IV.) Ähnlich, wie die Gleichung III) wird auch die allgemeinere

Gleichung: $\qquad \varphi(x) = 2^n q^m$

aufgelöst. Wir setzen zu diesem Zwecke

$$p_1 - 1 = 2^{n-\nu} . q^{m-\mu}, \text{ worin } \nu < n,\ \mu < m \text{ ist.}$$

Dann muss also: $p_1 = 2^{n-\nu} . q^{m-\mu} + 1$ eine Primzahl sein.

Die aufzulösende Gleichung nimmt folgende Gestalt an:

$$p_2^{\alpha_2 - 1} . . (p_2 - 1) . . . = \varphi(y) = 2^\nu q^\mu \quad . \quad . \quad . \quad 8)$$

Kennt man eine Auflösung dieser Gleichung z. B. $y = a$, so ist $x = a\,p$ eine Lösung der Gl. IV) Für zwei besondere Fälle haben wir die Auflösung dieser Gleichung schon gefunden, nämlich für $\mu = 0$ und $\mu = 1$. Wir nehmen daher jetzt an:

a) Es sei $\mu > 1$, dann muss $\nu > 0$ sein, weil sonst auf der rechten Seite eine ungerade Zahl stände, somit die Aufgabe unmöglich wäre.

Da die Gl. 8) die nämliche Form wie die vorgelegte hat und sich von derselben nur durch die Größe der Exponenten unterscheidet, so wenden wir auf sie dasselbe Verfahren wie oben an, d. h. wir setzen:

$$p_2 - 1 = 2^{\nu - \nu_1} q^{\mu - \mu_1}, \quad \text{wobei} \quad \nu_1 < \nu \quad \text{und} \quad \mu_1 < \mu \quad \text{sein soll.}$$

Durch Einsetzung des Wertes $p_2 = 2^{\nu - \nu_1} q^{\mu - \mu_1} + 1$, der eine Primzahl sein muss, erhalten wir eine Gleichung von der Form:

$$p_3^{\alpha_3 - 1} . . (p_3 - 1) . . = \varphi(y_1) = 2^{\nu_1} q^{\mu_1}.$$

Für $\mu_1 = 0, 1$ kennen wir bereits die Lösung. Eine solche sei $y_1 = b$, dann ist $y = b\,p_2$ eine Lösung der Gl. 8) und $x = b\,p_2\,p_1$ eine Lösung der vorgelegten Gleichung, wenn $p_2 \gtrless p_1$ ist.

Für $\mu_1 > 1$ wenden wir das eben angegebene Verfahren abermals an, wodurch in der Lösung eine neue Primzahl auftritt. Auf diese Weise lassen sich alle für μ möglichen Fälle erledigen.

b) Es kann auch $\mu = m$ sein, wenn $q = 2^{2^\lambda} + 1$ und $2^\lambda < n$ ist. In diesem Falle erhalten wir noch Auflösungen von der Form;

$$x = c\,q^{m+1},$$

worin c eine Lösung der Gleichung: $\varphi\,(z) = 2^{n - 2^\lambda}$ bedeutet.

Zusatz: Eine Zahl von der Form $2^n q^m + 1$, worin $q > 3$ ist, ist keine Primzahl, sondern durch 3 theilbar in folgenden drei Fällen:

1) Wenn $n = 2\nu + 1$, $m = 2\mu$ und $q = 6k \pm 1$
2) „ $n = 2\nu + 1$, $m = 2\mu + 1$ „ $q = 6k + 1$
3) „ $n = 2\nu$, $m = 2\mu + 1$ „ $q = 6k - 1$

Daher kann eine Zahl von der obigen Form nur dann eine Primzahl sein, wenn

1) $n = 2\nu$, $m = 2\mu$ und $q = 6k \pm 1$
2) $n = 2\nu$, $m = 2\mu + 1$ „ $q = 6k + 1$
3) $n = 2\nu + 1$, $m = 2\mu + 1$ „ $q = 6k - 1$ ist.

Wir haben nun alle Fälle erledigt, in denen außer 2 nur noch eine einzige ungerade Primzahl vorkommt. Im Folgenden haben wir uns mit solchen Zahlen zu beschäftigen, in denen zwei oder mehrere ungerade Primfactoren erscheinen.

Wir werden auch hier wiederum mit dem einfachsten Falle beginnen.

V) Es sei $\varphi\,(x) = 2\,q\,r$ und $r > q$

Setzen wir *a)* $p_1 - 1 = 2\,q\,r$ also $p_1 = 2\,q\,r + 1$,
so erhalten wir als Auflösungen:

$$x_1 = 2\,q\,r + 1 \quad \text{und} \quad x_2 = 2\,(2\,q\,r + 1).$$

Setzen wir aber *b)* $p_1 - 1 = 2\,q$, also $p_1 = 2\,q + 1$,
so muss $2\,q + 1 = r$ und $\alpha_1 = 2$ sein,
wodurch wir die Lösungen: $x_3 = r^2$ und $x_4 = 2\,r^2$ erhalten.

Wir können somit sagen:

Die Gleichung: $\varphi\,(x) = 2\,q\,r$ hat.

a) gar keine Lösung, wenn weder $2qr + 1$ eine Primzahl, noch $r = 2q + 1$ ist;

b) zwei Lösungen, wenn $\alpha)$ $2qr + 1$ eine Primzahl ist und $r \gtrless 2q + 1$, nämlich:

$$x_1 = 2\,q\,r + 1 \text{ und } x_2 = 2\,(2\,q\,r + 1),$$

$\beta)$ $2qr + 1$ keine Primzahl, aber $r = 2q + 1$ ist, nämlich $x_1 = (2q+1)^2$ und $x_2 = 2\,(2q+1)^2$;

c) vier Lösungen, wenn sowohl $2qr+1$ eine Primzahl, als auch $r=2q+1$ ist.

Die Lösungen haben die unter α) und β) angegebenen Formen.

VI.) Ist $\varphi(x) = 2q^n r,$ so setzen wir:

a) $p_1 - 1 = 2q^{n-\nu} r$. Die aufzulösende Gleichung heisst dann:

$$\left(2q^{n-\nu} r + 1\right)^{\alpha_1 - 1} p_2^{\alpha_2 - 1} (p_2 - 1) = q^\nu.$$

Diese Gleichung ist, weil $2q^{n-\nu} r + 1$ relativ prim zu q ist, nur dann möglich, wenn $\nu = 0$, $\alpha_1 = 1$ ist; dann erhalten wir:

$$x_1 = 2q^n r + 1 \quad \text{und} \quad x_2 = 2\left(2q^n r + 1\right).$$

b) $p_1 - 1 = 2q^{n-\nu}$; dann muss $\left(2q^{n-\nu} + 1\right)^{\alpha_1 - 1} p_2^{\alpha_2 - 1} (p_2 - 1) = q^\nu r$ sein.

Diese ist nur möglich, wenn $\nu = 0$, $r = 2q^n + 1$ und $\alpha_1 = 2$ ist. Hat also die gegebene Gleichung die Form: $\varphi(x) = 2q^n\left(2q^n + 1\right)$, so gibt es folgende zwei Lösungen: $x_1 = \left(2q^n + 1\right)^2$ und $x_2 = 2\left(2q^n + 1\right)^2$.

c) $p_1 - 1 = 2r$, so muss: $(2r+1)^{\alpha_1 - 1} p_2^{\alpha_2 - 1} (p_2 - 1) = q^n$ sein.
Diese ist erfüllt für: $q = 2r + 1$, $\alpha_1 = n + 1$.
Die Lösungen haben die Form: $x_1 = (2r+1)^{n+1}$ und $x_2 = 2(2r+1)^{n+1}$.
Da die beiden Fälle *b*) und *c*) einander ausschließen, so können nicht beide gleichzeitig eintreten.

Zu ganz denselben Ergebnissen führt die Gleichung:

$$\varphi(x) = 2q^n r^s.$$

Die Lösungen dieser Gleichung sind:

a) Wenn $2q^n r^s + 1$ eine Primzahl ist,

$$x = 2q^n r^s + 1 \quad \text{und} \quad x = 2\left(2q^n r^s + 1\right);$$

b) wenn $r = 2q^n + 1$ ist,

$$x = \left(2q^n + 1\right)^{s+1} \quad \text{und} \quad x = 2\left(2q^n + 1\right)^{s+1};$$

c) wenn $q = 2r^s + 1$ ist,

$$x = \left(2r^s + 1\right)^{n+1} \quad \text{und} \quad x = 2\left(2r^s + 1\right)^{n+1}.$$

VII.) Wenn $\varphi(x) = 2^m q r,$ so setzen wir:

a) $p_1 = 2^{m-\mu} q r + 1,$ worin $\mu < m$ sein muss.

Dann ist $x = a\left(2^{m-\mu} q r + 1\right)$ eine Lösung der vorgelegten Gleichung, wobei a eine Lösung der Gleichung $\varphi(y) = 2^\mu$ ist.

b) $p_1 = 2^{m-\mu} q + 1$; dann muss:

$$\left(2^{m-\mu} q + 1\right)^{\alpha_1 - 1} p_2^{\alpha_2 - 1} (p_2 - 1) \ldots = 2^{\mu} r \text{ und } \mu > 0 \text{ sein.}$$

α) Für $\alpha_1 = 1$ muss $\varphi(y) = 2^{\mu} r$ sein. Ist $y = b$ eine Lösung dieser Gleichung, so ist $x = b\left(2^{m-\mu} q + 1\right)$ eine Lösung unserer Aufgabe, vorausgesetzt, dass b relativ prim zu p_1 ist.

β) Ist speciell: $r = 2^{m-\mu} q + 1$, so muss $\alpha = 2$ und $\varphi(z) = 2^{\mu}$ sein. Ist nun $z = c$, so ist $x = c\, r^2$, wenn c relativ prim zu r ist.

Dieselben Untersuchungen, wie für die Primzahl q, müssen auch für die Primzahl r angestellt werden.

c) $p_1 = 2^{m-\mu} + 1$, dann muss:

$$\left(2^{m-\mu} + 1\right)^{\alpha_1 - 1} . p_2^{\alpha_2 - 1} (p_2 - 1) \ldots = 2^{\mu} q\, r \text{ und } \mu > 0 \text{ sein.}$$

α) Wenn nun $q = 2^{m-\mu} + 1$ ist, so muss $\alpha_1 = 2$ und $\varphi(y) = 2^{\mu} r$ sein. Da $m - \mu$ von der Form 2^{λ} sein muss, so ist $\mu = m - 2^{\lambda}$, also

$$\varphi(y) = 2^{m - 2^{\lambda}} r \text{ und } 2^{\lambda} < m \quad \text{Für } y = a, \text{ ist } x = a\, q^2.$$

β) Ebenso kann auch $r = 2^{m-\mu} + 1$ gesetzt werden, wodurch wir Lösungen von der Form $x = b\, r^2$ erhalten.

VIII.) Ist endlich die allgemeine Gleichung:

$$\varphi(x) = 2^m q^n r^s \ldots$$

aufzulösen, so setzen wir:

$$p_1 = 2^{m-\mu} q^{n-\nu} r^{s-\sigma} \ldots + 1,$$

wobei $\mu < m, \quad \nu \overline{<} n, \quad \sigma \overline{<} s \ldots$ sein kann.

Wir haben dann alle möglichen Werte von μ mit allen möglichen Werten von ν, σ . . . zu combinieren, wodurch wir Gleichungen von der Form:

$$\varphi(y) = 2^{\mu} q^{\nu} r^{\sigma} \ldots$$

erhalten. Für einzelne specielle Fälle haben wir die Lösungen derselben bereits in den vorhergehenden Abschnitten gefunden. Auf die übrigen wenden wir dann abermals dasselbe Verfahren wie oben an, wodurch die Exponenten neuerdings herabgedrückt werden, so dass also immer nur Gleichungen von einer schon behandelten Form aufzulösen sind.

Damit haben wir nun unsere Aufgabe vollständig gelöst. Wir ersehen aus den vorhergehenden Erörterungen, dass es schließlich immer auf die Auflösung einer Gleichung von der Form: $\varphi(x) = 2^n$ ankommt.

Auf die voranstehend gelöste Aufgabe lässt sich auch die folgende Aufgabe zurückführen:

Es sind diejenigen Zahlen n zu finden, für welche die Summe der $\varphi(n)$ Zahlen ein gegebenes Vielfaches von n ist.

Die Summe s derjenigen $\varphi(n)$ Zahlen, welche relativ prim zu n und kleiner als n sind, ist gegeben durch die Formel:

$$s = n\,\frac{\varphi(n)}{2}, \quad \text{wenn} \quad n > 1 \quad \text{ist.}$$

Soll nun $s = kn$ sein, so muss $kn = n\,\frac{\varphi(n)}{2}$ sein; somit kommt es auf die Auflösung der Gleichung an:

$$\varphi(n) = 2k,$$

worin k eine gegebene Zahl bezeichnet.

Z. B.: Für welche Zahlen n ist die Summe der $\varphi(n)$ Zahlen gleich der Zahl n selbst?

Es soll also:

$$\frac{n}{2}\,\varphi(n) = n, \quad \text{daher} \quad \varphi(n) = 2 \quad \text{sein.}$$

Dies ist der Fall, wenn $n = 3,\ 4,\ 6$ ist.

In der Tabelle am Schlusse sind die Lösungen der Gleichung $\varphi(x) = n$ für alle möglichen Werte von n bis einschließlich $n = 200$ zusammengestellt. Die Lösungen bis zu $n = 100$ sind dem Werke „Théorie des nombres von Ed. Lucas" entnommen; darin ist aber keine Andeutung über die Berechnung dieser Zahlen enthalten. Die übrigen Lösungen sind vom Verfasser dieses Aufsatzes berechnet worden. Die mit ν überschriebene Columne gibt die Anzahl der Lösungen an.

Tafel

der Zahlen, welche einem gegebenen Werte von $\varphi(n)$ entsprechen.

$\varphi(n)$	n	ν
1	1, 2.	2
2	3, 4, 6.	3
4	5, 8, 10, 12.	4
6	7, 9, 14. 18.	4
8	15, 16, 20, 24, 30	5
10	11, 22.	2
12	13, 21, 26 28, 36, 42.	6
16	17, 32, 34, 40, 48, 60.	6
18	19, 27, 38, 54.	4
20	25, 33 44, 50, 66.	5
22	23, 46.	2
24	35, 39, 45, 52, 56, 70, 72, 78, 84, 90.	10
28	29, 58.	2
30	31, 62.	2

φ (n)	n	ν
32	51, 64, 68, 80, 96, 102, 120.	7
36	37, 57, 63, 74, 76, 108, 114, 126.	8
40	41, 55, 75, 82, 88, 100, 110, 132, 150.	9
42	43, 49, 86, 98.	4
44	69, 92, 138.	3
46	47, 94.	2
48	65, 104, 105, 112, 130, 140, 144, 156, 168, 180, 210.	11
52	53, 106.	2
54	81, 162.	2
56	87, 116, 174.	3
58	59, 118	2
60	61, 77, 93, 99, 122, 124, 154, 186, 198	9
64	85, 128, 136, 160, 170, 192, 204, 240.	8
66	67, 134.	2
70	71, 142.	2
72	73, 91, 95, 111, 117, 135, 146, 148, 152, 182, 190, 216, 222, 228, 234, 252, 270.	17
78	79, 158.	2
80	123, 164, 165, 176, 200, 220, 246, 264, 300, 330.	10
82	83, 166.	2
84	129, 147, 172, 196, 258, 294.	6
88	89, 115, 178, 184, 230, 276.	6
92	141, 188, 282.	3
96	97, 119, 153, 194, 195, 208, 224, 238, 260, 280, 288, 306, 312, 336, 360, 390, 420.	17
100	101, 125, 202, 250.	4
102	103, 206.	2
104	159, 212, 318.	3
106	107, 214.	2
108	109, 133, 171, 189, 218, 266, 324, 342, 378	9
110	121, 242.	2
112	113, 145, 226, 232, 290, 348	6
116	177, 236, 354.	3
120	143, 155, 175, 183, 225, 231, 244, 248, 286, 308, 310, 350, 366, 372, 396, 450, 462.	17
126	127, 254.	2
128	255, 256, 272, 320, 340, 384, 408, 480, 510	9
130	131, 262.	2
132	161, 201, 207, 268, 322, 402, 414.	7
136	137, 274.	2
138	139, 278.	2
140	213, 284, 426.	3
144	185, 219, 273, 285, 292, 296, 304, 315, 364, 370, 380, 432, 438, 444, 456, 468, 504, 540, 546, 570, 630.	21
148	149, 298.	2
150	151, 302.	2

φ (n)	n	ν
156	157, 169, 237, 314, 316, 338, 474.	7
160	187, 205, 328, 352, 374, 400, 410, 440, 492, 528, 600, 660.	12
162	163, 243, 326, 486.	4
164	249, 322, 498.	3
166	167, 334.	2
168	203, 215, 245, 261, 344, 392, 406, 430, 490, 516, 522, 588.	12
172	173, 346.	2
176	267, 345, 356, 368, 460, 534, 552, 690.	8
178	179, 358.	2
180	181, 209, 217, 279, 297, 362, 418, 434, 558, 594.	10
184	235, 376, 470, 564.	4
190	191, 382.	2
192	193, 221, 291, 357, 386, 388, 416, 442, 448, 476, 520, 560, 576, 582, 612, 624, 672, 714, 720, 780, 840.	21
196	197, 394.	2
198	199, 398.	2
200	275, 303, 375, 404, 500, 550, 606, 750.	8