PRIMITIVE WURZELN DER PRIMZAHLEN VON DER FORM $2^{\varkappa}q^{\lambda}+1$, IN WELCHER $q=1$ ODER EINE UNGERADE PRIMZAHL IST

VON

G. WERTHEIM

in FRANKFURT a. M.

Wenn die Primzahl $p = 2^{\varkappa}q^{\lambda}\dots r^{\mu}+1$ ist, wo $\varkappa, \lambda, \dots, \mu$ ganze positive Zahlen, $q, \dots, r$ von einander verschiedene ungerade Primzahlen bezeichnen, so ist bekanntlich die Zahl a eine primitive Wurzel von p, wenn keine der Congruenzen

$$x^2 \equiv a, \qquad x^q \equiv a\ , \ \dots\ , \ x^r \equiv a \ (\text{mod. } p)$$

möglich ist. Die Untersuchung, ob a primitive Wurzel von p sei oder nicht, wird sich also um so einfacher gestalten, je weniger ungleiche Primfactoren $p-1$ enthält. Es sei nun

I. $$p = 2^{\varkappa}+1.$$

In diesem Falle ist a primitive Wurzel von p, wenn die Congruenz $x^2 \equiv a$ (mod. p) unmöglich, d. h. wenn a quadratischer Nichtrest von p ist. Wir denken uns jetzt die Zahlen der Form $2^{\varkappa}+1$ in folgender Weise geordnet:

$$2^1+1\ ,\ 2^3+1\ ,\ 2^5+1\ ,\ \dots$$
$$2^2+1\ ,\ 2^6+1\ ,\ 2^{10}+1\ ,\ \dots$$
$$2^4+1\ ,\ 2^{12}+1\ ,\ 2^{20}+1\ ,\ \dots$$
$$2^8+1\ ,\ 2^{24}+1\ ,\ 2^{40}+1\ ,\ \dots$$
$$\dots\dots\dots\dots\dots\dots$$

Acta mathematica. 20. Imprimé le 17 décembre 1895.

Da das erste Glied jeder dieser Horizontalreihen in jedes folgende Glied derselben Reihe ohne Rest aufgeht, so sind die Primzahlen der Form $2^x + 1$ nur unter den ersten Gliedern zu suchen; mit anderen Worten: Nur wenn x eine Potenz von 2 ist, kann $2^x + 1$ eine Primzahl sein. Dass aber nicht alle Zahlen $2^x + 1$, bei denen x eine Potenz von 2 ist, auch Primzahlen seien, wie FERMAT vermuthet hatte, ist von EULER gezeigt worden.

Wenn wir jetzt von den beiden Primzahlen $2^1 + 1 = 3$, $2^2 + 1 = 5$, von denen die erste die primitive Wurzel 2, die zweite die primitiven Wurzeln 2 und 3 hat, absehen, so ergiebt sich Folgendes: Es ist congruent

	mod. 8	mod. 12	mod. 20	mod. 28	mod. 44	mod. 52	...
2^4	0	4	16	16	16	16	...
2^8	0	4	16	4	36	48	...
2^{16}	0	4	16	16	20	16	...
2^{32}	0	4	16	4	4	48	...
.	.	.	.	.	.	.	

Folglich haben die Primzahlen $2^x + 1$, $x > 3$ die Formen $8k + 1$; $12k + 5$; $20k + 17$; $28k + 5, 17$; $44k + 5, 17, 21, 37$; $52k + 17, 49$; ..., und da 2 quadratischer Rest der Primzahlen $8k + 1$, 3 Nichtrest der Primzahlen $12k + 5$, 5 Nichtrest der Primzahlen $20k + 17$, 7 Nichtrest der Primzahlen $28k + 5, 17$, ferner 13 Rest der Primzahlen $52k + 17, 49$ ist, während 11 Rest der Primzahlen $44k + 5, 37$, Nichtrest der Primzahlen $44k + 17, 21$ ist, so erhalten wir den Satz:

Die Zahlen 3, 5, 7 *sind primitive Wurzeln aller Primzahlen* $2^x + 1$, $x > 3$; *die Zahlen* 2 *und* 13 *sind für keine derselben primitive Wurzeln; die Zahl* 11 *endlich ist primitive Wurzel derjenigen dieser Primzahlen, bei denen* x *eine gerade Potenz von* 2 *ist; wenn* x *eine ungerade Potenz von* 2 *ist, so ist* 11 *keine primitive Wurzel.*

Unter 10000 liegen nur 4 Primzahlen der Form $2^x + 1$, nämlich 3, 5, 17, 257.

Weiter sei

II. $$p = 2^x q^\lambda + 1;$$

dann ist die Zahl a primitive Wurzel von p, wenn sie Nichtrest von p und wenn zugleich die Congruenz

$$x^q \equiv a, \quad \text{also auch} \quad x^{q.2^x q^{\lambda-1}} \equiv a^{2^x q^{\lambda-1}} \pmod{p}$$

unmöglich ist. Nach dem Fermat'schen Satze ist aber

$$x^{q.2^x q^{\lambda-1}}, \quad \text{d. i.} \quad x^{p-1} \equiv 1 \pmod{p};$$

also muss, wenn a primitive Wurzel sein soll, auch die Congruenz

$$a^{2^x q^{\lambda-1}} \equiv 1, \quad \text{d. i.} \quad (a^{2^{x-1} q^{\lambda-1}} - 1)(a^{2^{x-1} q^{\lambda-1}} + 1) \equiv 0 \pmod{p}$$

unmöglich sein.

Wenn nun $\lambda > 1$ ist, so kann die Frage, ob der Nichtrest a primitive Wurzel von p sei oder nicht, nur dadurch entschieden werden, dass man den Rest der Potenz $a^{2^{x-1} q^{\lambda-1}} \pmod{p}$ bildet; wenn derselbe weder $+1$ noch -1 ist, so ist a primitive Wurzel, sonst nicht.

Beispiel. Es sei $p = 3457 = 2^7 . 3^3 + 1$, so ist $2^{x-1} q^{\lambda-1} = 2^6 . 3^2 = 576$. Nun sind $2, 3, 6$ Reste von 3457; weiter ergiebt sich $5^{576} \equiv -1$, aber $7^{576} \equiv -1520 \pmod{3457}$; somit ist 7 die kleinste primitive Wurzel von 3457.

Unter 10000 liegen 27 Primzahlen der Form $2^x q^\lambda + 1$, $\lambda > 1$, deren kleinste primitive Wurzeln auf die dargelegte Weise leicht bestimmt werden können.

Weit einfacher gestaltet sich die Sache, wenn $\lambda = 1$, also $q^{\lambda-1} = 1$ ist. In diesem Falle entnehmen wir aus dem oben erhaltenen Resultat den Satz:

Die Zahl a ist primitive Wurzel der Primzahl $p = 2^x q + 1$, wenn sie Nichtrest von p und wenn zugleich $a^{2^x} - 1$ nicht durch p teilbar ist.

Dieser Satz soll jetzt auf besondere Fälle angewendet werden.

1) Es sei $x = 1$, also $p = 2q + 1$.

Je nachdem dann $q = 4k + 1$ oder $= 4k + 3$ ist, ist $p = 8k + 3$ oder $= 8k + 7$. Da nun die Zahl $a = 2$ Nichtrest von $p = 8k + 3$, dagegen Rest von $8k + 7$ ist, da ausserdem $2^2 - 1 = 3$ durch keine Primzahl $p = 2q + 1$, $q > 1$ teilbar ist, so erhalten wir das Resultat:

Die Zahl 2 ist primitive Wurzel aller Primzahlen $p = 2q + 1$, bei denen die ungerade Primzahl q die Form $4k + 1$ hat; wenn $q = 4k + 3$ ist, so ist 2 keine primitive Wurzel von p.

Um weiter zu untersuchen, für welche Primzahlen $p = 2q + 1$ die Zahl $a = 3$ primitive Wurzel ist, erwägen wir, dass q entweder $= 3$ oder von einer der beiden Formen $6k \pm 1$ ist. Für $q = 3$ ist $p = 7$, und für diese Zahl ist 3 primitive Wurzel. Die Annahme $q = 6k + 1$ würde $p = 12k + 3$, also zusammengesetzte Zahlen liefern und ist daher unzulässig. Wenn endlich $q = 6k - 1$ ist, so ergiebt sich $p = 12k - 1$, und da 3 Rest der Primzahlen dieser Form ist, so erhalten wir den Satz:

Die Zahl 3 ist primitive Wurzel von 7; für alle anderen Primzahlen $p = 2q + 1$ ist sie es nicht.

Durch ähnliche Schlüsse und unter Berücksichtigung der Werte

$$5^2 - 1 = 24, \quad 6^2 - 1 = 35, \quad 7^2 - 1 = 48, \quad 10^2 - 1 = 99,$$

$$11^2 - 1 = 120, \quad 13^2 - 1 = 168, \quad \ldots$$

gelangt man zu den Sätzen:

5 *ist primitive Wurzel aller Primzahlen $2q + 1$, bei denen q eine Primzahl einer der beiden Formen $10k + 1, 3$ ist.*

6 *ist primitive Wurzel aller Primzahlen $2q + 1$, bei denen q eine Primzahl der Form $4k + 1$ ist.*

7 *ist primitive Wurzel aller Primzahlen $2q + 1$, bei denen q eine Primzahl einer der beiden Formen $14k + 5, 11$ ist.*

10 *ist primitive Wurzel aller Primzahlen $2q + 1$, bei denen q eine Primzahl einer der drei Formen $20k + 3, 9, 11$ ist.*

11 *ist primitive Wurzel aller Primzahlen $2q + 1$, bei denen q eine Primzahl einer der Formen $22k + 1, 7, 13, 15$ ist; ausserdem ist 11 primitive Wurzel von 23.*

13 *ist primitive Wurzel aller Primzahlen* $2q + 1$, *bei denen* q *eine Primzahl einer der Formen* $26k + 3, 5, 7, 9, 15, 23$ *ist. Ausnahme* $p = 7$.

Diese Sätze, denen sich leicht andere anreihen lassen, liefern für 113 von den 114 unter 10000 liegenden Primzahlen $2q + 1$ die kleinsten primitiven Wurzeln; die eine noch übrig bleibende Primzahl 2999 hat 17 als kleinste primitive Wurzel.

Ist

$$2) \qquad x = 2, \text{ also } p = 4q + 1,$$

so wird, je nachdem $q = 4k + 1$ oder $4k + 3$ ist, p die Form $16k + 5$ oder $16k + 13$ haben, und da 2 Nichtrest der Primzahlen dieser Form ist, da überdies $2^4 - 1 = 15$ durch keine Primzahl $4q + 1$, $q > 1$ teilbar ist, so ergiebt sich der Satz:

Die Zahl 2 *ist primitive Wurzel aller Primzahlen* $4q + 1$, *bei denen* q *eine ungerade Primzahl ist.*

Indem wir diese Schlüsse fortsetzen und beachten, dass $3^4 - 1 = 80$, $6^4 - 1 = 1295 = 5 \cdot 7 \cdot 37$, $7^4 - 1 = 2400$, $10^4 - 1 = 9999 = 9 \cdot 11 \cdot 101$, $11^4 - 1 = 14640 = 2^4 \cdot 3 \cdot 5 \cdot 61$, $13^4 - 1 = 28560 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17$ durch keine Primzahl der betrachteten Form teilbar sind, dass aber $5^4 - 1 = 624$ den Factor 13 enthält, erhalten wir die Sätze:

3 *ist primitive Wurzel aller Primzahlen* $4q + 1$ *mit Ausnahme der Zahl* 13.

5 *ist primitive Wurzel aller Primzahlen* $4q + 1$, *bei denen* q *eine Primzahl einer der Formen* $10k + 3, 9$ *ist; eine Ausnahme macht nur die Zahl* 13.

6 *ist primitive Wurzel von* 13; *für alle anderen Primzahlen* $4q + 1$ *ist* 6 *keine primitive Wurzel.*

7 *ist primitive Wurzel aller Primzahlen* $4q + 1$, *bei denen* q *eine Primzahl einer der Formen* $14k + 1, 3, 11$ *ist.*

10 *ist primitive Wurzel der Primzahlen* $4q + 1$, *bei denen* q *eine Primzahl der Form* $10k + 7$ *ist.*

11 *ist primitive Wurzel der Primzahlen* $4q + 1$, *bei denen* q *eine Primzahl einer der Formen* $22k + 3, 5, 7, 15, 21$ *ist.*

Unter 10000 liegen 59 Primzahlen der vorstehend betrachteten Form.

Wenn endlich

3) $x > 2$ ist, so hat $p = 2^x q + 1$ die Form $8k + 1$, und da 2 Rest der Primzahlen dieser Form ist, so erhalten wir den Satz:

Die Zahl 2 ist für keine Primzahl $2^x q + 1$, $x > 2$ primitive Wurzel.

Ebenso liefert eine einfache Anwendung des Reciprocitätssatzes das Resultat:

Für die Primzahlen $2^x q + 1$, $x > 2$ kann weder q noch $2q$ primitive Wurzel sein.

Danach ist z. B. weder 3 noch 6 primitive Wurzel der Primzahlen $2^x . 3 + 1$, weder 5 noch 10 primitive Wurzel der Primzahlen $2^x . 5 + 1$, u. s. w.

Untersuchen wir jetzt, für welche Primzahlen $2^x q + 1$, $x > 2$ die Zahl 3 primitive Wurzel sei. Da der Fall $q = 3$ soeben erledigt worden ist, so haben wir nur $q = 6k \pm 1$ vorauszusetzen. Für diese Werthe wird

$$p = 2^x . 6k \pm 2^x + 1 \equiv \pm 2^x + 1 \pmod{12}.$$

Nun ist aber, da $x > 2$ vorausgesetzt wird,

$$2^x \equiv 4 \text{ oder } 8 \pmod{12},$$

folglich wird, wenn das obere Zeichen genommen wird, $p \equiv 5$ oder 9 und für das untere Zeichen $p \equiv -3$ oder -7, das ist $\equiv 9$ oder 5 (mod. 12) sein. Da nun p eine Primzahl sein soll, so ist der Rest 9 ausgeschlossen; folglich hat *jede* Primzahl $2^x q + 1$, $x > 2$, $q > 3$ die Form $12k + 5$, also 3 zum Nichtrest.

Die Zahl 3 ist daher primitive Wurzel aller Primzahlen $2^x q + 1$, $x > 2$, $q > 3$, welche nicht in $3^{2^x} - 1$ aufgehen. Es ist aber $3^8 - 1 = 2^5 . 5 . 41$ und $3^{16} - 1 = 2^6 . 5 . 17 . 41 . 193$. Daraus ergeben sich die Sätze:

3 *ist primitive Wurzel aller Primzahlen $8q + 1$, mit Ausnahme der Zahl 41.*

3 *ist primitive Wurzel aller Primzahlen $16q + 1$.*

Ebenso ist 3 primitive Wurzel aller Primzahlen $32q + 1$, welche nicht in $3^{32} - 1$ aufgehen, aller Primzahlen $64q + 1$, welche nicht in

$3^{64} - 1$ aufgehen, u. s. w. Um die (praktisch unausführbare) Zerlegung dieser Ausdrücke in Faktoren oder die Division derselben durch alle in Betracht kommenden Primzahlen des Gebiets, auf welches man sich beschränkt, zu vermeiden, berechnet man am besten die Potenzreste von 3 für jede dieser Primzahlen p bis zu $3^{\frac{1}{2}\varphi(p-1)}$. Wenn dies die niedrigste Potenz ist, welche den Rest -1 liefert, so ist 3 primitive Wurzel von p, sonst nicht. Auf diese Weise habe ich mich überzeugt, dass für das Zahlengebiet bis zu 10000 alle Primzahlen $2^x q + 1$, $x > 2$, $q > 3$ in der That die primitive Wurzel 3 haben.

Anmerkung. $3^{2^x} - 1 = (3^{2^{x-1}} + 1)(3^{2^{x-1}} - 1)$ wird durch die Primzahl $p = 2^x q + 1$ sicherlich nicht teilbar sein, wenn

$$2^x q + 1 > 3^{2^{x-1}} + 1, \quad \text{also} \quad q > \frac{3^{2^{x-1}}}{2^x}$$

ist. Unter dieser Bedingung ist also 3 primitive Wurzel von p. Dieser von TSCHEBYSCHEFF (*Theorie der Congruenzen*, deutsch von SCHAPIRA, S. 311) angegebene Grenzwert ist aber nur für $x = 3$ von Nutzen; er liefert dann $q > \frac{3^4}{2^3}$, d. i. $q > 10$. Für $x = 4$ wird derselbe $q > 410$; von den 17 unter 10000 liegenden Primzahlen $16q + 1$ würden also nur die 4 letzten 7793, 8369, 8753, 9137 unter den Satz fallen, die 13 ersten nicht. Für $x = 5$ ist der Grenzwert $q > 1345210$, für $x = 6$, u. s. w. noch weit grösser. Dieser Grenzwert hat also praktisch gar keine Bedeutung.

Es sei jetzt $a = 5$. Da der Fall $q = 5$ oben schon erledigt ist, so sind nur die Formen

$$q = 10k + 1, 3, 7, 9$$

ins Auge zu fassen, denen die Werte

$$p = 10.2^x.k + (2^x + 1), (3.2^x + 1), (7.2^x + 1), (9.2^x + 1)$$

entsprechen. Je nachdem nun

$$x(> 2) \equiv 0, 1, 2, 3 \pmod 4$$

ist, wird (mod. 10)

$$2^x \equiv 6, 2, 4, 8,$$

also

$$2^x + 1 \equiv 7, 3, 5, 9,$$

$$3 \cdot 2^x + 1 \equiv 9, 7, 3, 5,$$

$$7 \cdot 2^x + 1 \equiv 3, 5, 9, 7,$$

$$9 \cdot 2^x + 1 \equiv 5, 9, 7, 3$$

sein, und da 5 Nichtrest der Primzahlen $10k + 3, 7$, Rest der Primzahlen $10k + 1, 9$ ist, so erhalten wir das Resultat:

Die Zahl 5 ist Nichtrest der Primzahlen

$2^{4\lambda}q + 1$, wenn die Primzahl q eine der Formen $10k + 1, 7$ hat.

$2^{4\lambda+1}q + 1$, » » » q » » » $10k + 1, 3$ »

$2^{4\lambda+2}q + 1$, » » » q » » » $10k + 3, 9$ »

$2^{4\lambda+3}q + 1$, » » » q » » » $10k + 7, 9$ »

Zur Entscheidung der Frage, ob die Zahl 5 primitive Wurzel derjenigen Primzahlen $2^x q + 1$ sei, deren Nichtrest sie ist, hat man dann noch die Ausdrücke

$$5^8 - 1 = 2^5 \cdot 3 \cdot 13 \cdot 313, \qquad 5^{16} - 1 = 2^6 \cdot 3 \cdot 13 \cdot 17 \cdot 313 \cdot 11489, \quad \ldots$$

zu prüfen und, wenn dies unmöglich ist, die Potenzreste von 5 selbst zu bilden. Im besonderen erhält man die Sätze:

5 *ist primitive Wurzel aller Primzahlen* $8q + 1$, *wenn* q *eine Primzahl einer der Formen* $10k + 7, 9$ *ist.*

5 *ist primitive Wurzel aller Primzahlen* $16q + 1$, *wenn* q *eine Primzahl einer der Formen* $10k + 1, 7$ *ist.*

Weiter sei $a = 6$. Da 2 Rest, 3 Nichtrest aller Primzahlen $2^x q + 1$, $x > 2$, $q > 3$ ist, so ist 6 Nichtrest derselben. Nun ist

$$6^8 - 1 = 5 \cdot 7 \cdot 37 \cdot 1297, \qquad 6^{16} - 1 = 5 \cdot 7 \cdot 17 \cdot 37 \cdot 1297 \cdot 98801,$$

somit 6 *primitive Wurzel aller Primzahlen* $8q + 1$ *und* $16q + 1$. Was die Primzahlen $32q + 1, 64q + 1, \ldots$ betrifft, so ist die Frage in der oben dargelegten Weise zu entscheiden.

Für $a = 7$ sind die Fälle

$$q = 14k + 1, 3, 5, 9, 11, 13$$

zu betrachten, denen die Werte

$$p = 14.2^x k + (2^x + 1), (3.2^x + 1), (5.2^x + 1), (9.2^x + 1), (11.2^x + 1), (13.2^x + 1)$$

entsprechen. Je nachdem nun

$$x \equiv 0, 1, 2 \pmod 3$$

ist, wird mod. 28

$$2^x \equiv 8, 16, 4,$$

also

$$2^x + 1 \equiv 9, 17, 5,$$
$$3.2^x + 1 \equiv 25, 21, 13,$$
$$5.2^x + 1 \equiv 13, 25, 21,$$
$$9.2^x + 1 \equiv 17, 5, 9,$$
$$11.2^x + 1 \equiv 5, 9, 17,$$
$$13.2^x + 1 \equiv 21, 13, 25$$

sein, und da 7 Nichtrest der Primzahlen $28k + 5, 11, 13, 15, 17, 23$, Rest der übrigen ist, so erhalten wir das Resultat:

Die Zahl 7 ist Nichtrest der Primzahlen

$2^{3\lambda} q + 1$, wenn die Primzahl q von einer der Formen $14k + 5, 9, 11$ ist.

$2^{3\lambda+1} q + 1$, » » » q » » » » $14k + 1, 9, 13$ »

$2^{3\lambda+2} q + 1$, » » » q » » » » $14k + 1, 3, 11$ »

Zur Entscheidung der Frage, ob 7 primitive Wurzel derjenigen dieser Primzahlen sei, deren Nichtrest sie ist, sind dann noch die Ausdrücke

$$7^8 - 1 = 2^6 . 3 . 5^2 . 1201, \qquad 7^{16} - 1 = 2^7 . 3 . 5^2 . 11 . 13 . 29 . 683 . 1201$$

zu betrachten und weiter die Potenzreste von 7 selbst zu bilden. Im besonderen erhält man die Sätze:

7 ist primitive Wurzel der Primzahlen $8q+1$, *wenn die Primzahl* q *von einer der Formen* $14k+5, 9, 11$ *ist, und der Primzahlen* $16q+1$, *wenn* q *eine der Formen* $14k+1, 9, 13$ *hat.*

Die Zahl $a = 10$ ist in Beziehung auf die hier betrachteten Primzahlen $2^x q+1$ von demselben quadratischen Character wie 5, und da

$$10^8 - 1 = 3^2 . 11 . 73 . 101 . 137, \qquad 10^{16} - 1 = (10^8 - 1) . 17 . 5882353$$

ist, so ergeben sich die Sätze:

10 ist primitive Wurzel aller Primzahlen $8q+1$, *bei denen* q *eine Primzahl einer der beiden Formen* $10k+7, 9$ *ist; eine Ausnahme macht nur die Zahl* 137.

10 ist primitive Wurzel aller Primzahlen $16q+1$, *bei denen* q *eine Primzahl einer der beiden Formen* $10k+1, 7$ *ist.*