Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 18 (1945-1946)

Artikel: Über primitive Wurzeln von Primzahlen.
Autor: Fueter, Rud.
DOI: https://doi.org/10.5169/seals-16904

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 12.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Über primitive Wurzeln von Primzahlen

Von Rud. Fueter, Zürich

Einleitung.

Tschebyscheff hat als erster die Frage gestellt, für welche Primzahlen p eine gegebene Zahl primitive Wurzel sei, und als interessante Anwendung des *quadratischen Reziprozitätsgesetzes* Kriterien angegeben, die für 2 und 3 solche Primzahlen p festlegen[1]). Seine wesentlichen Resultate sagen aus, daß 3 primitive Wurzel aller Primzahlen der Gestalt $p=1+2^{2n}$ ist, und daß 2 primitive Wurzel aller Primzahlen der Gestalt $p=1+4q$ ist, wo q wieder eine Primzahl ist. *G. Wertheim* hat die Tschebyscheffsche Methode weiter ausgebaut und eine Reihe neuer Sätze erhalten[2]). Speziell hat er für 5, 6, 7, 10 und 11 Kriterien hergeleitet. Die spätere Arbeit von *Korkine* verfolgt dagegen andere Ziele[3]).

Man kann diese Resultate wesentlich verallgemeinern, wenn man statt des quadratischen das *kubische Reziprozitätsgesetz von Eisenstein* zu Hilfe nimmt. Man muß letzteres nur in der Form aussprechen, die *Leonhard Euler* schon ca. 1750 intuitiv gefunden hat, und die posthum publiziert worden ist. In der Vorrede zum Volumen 5 der ersten Serie der *Opera Omnia Leonhardi Euleri* habe ich ausgeführt, daß Eulers Vermutungen in der Tat Fälle des kubischen Reziprozitätsgesetzes enthalten[4]). Ich rekapituliere im ersten Paragraphen die Eulersche Fassung, soweit ich sie im zweiten und dritten benutzen muß.

1. Kubisches Reziprozitätsgesetz.

Bekanntlich kann man jede Primzahl p der Form $3n+1$ auf eine und nur eine Weise mittels natürlicher Zahlen x, y in der Gestalt

$$4p = x^2 + 27y^2 \tag{1}$$

darstellen. Aus ihr folgen die beiden weiteren Darstellungen:

---

[1]) *P. L. Tschebyscheff:* Theorie der Congruenzen (Elemente der Zahlentheorie) Dtsch. von Dr. H. Schapira, Berlin 1889, Anhang II, p. 306.

[2]) *G. Wertheim:* Primitive Wurzeln der Primzahlen von der Form $2^\kappa q^\lambda + 1$, in welcher $q = 1$ oder eine ungerade Primzahl ist. Acta mathematica, Bd. 20 (1897), p. 143.

[3]) Siehe *C. Posse:* Exposé succinct des résultats principaux du mémoire posthume de Korkine, avec une table des racines primitives et des caractères, qui s'y rapportent, calculée par lui pour les nombres premiers inférieurs à 4000 et prolongée jusqu'à 5000. Acta math. 35, p. 193.

[4]) *Leonhard Euler:* Opera Omnia, series I, vol. 5, Genf 1944, p. XXI u. ff.

$$4p = \left(\frac{x \pm 9y}{2}\right)^2 + 3\left(\frac{x \mp 3y}{2}\right)^2, \tag{2}$$

in denen die Basiszahlen der beiden Quadrate ebenfalls ganz sind. Nur in einer einzigen der drei Darstellungen (1) und (2) von $4p$ können beide Quadrate durch 4 gekürzt werden. Der kubische Restcharakter von 2, 3, 5, 7 wird jetzt nach Euler so gegeben:

2 *ist dann und nur dann kubischer Rest* (*mod.* p), *wenn in* (1) x *und* y *gerade sind.*

3 *ist dann und nur dann kubischer Rest* (*mod.* p), *wenn in* (1) y *durch* 3 *teilbar ist.*

5 *ist dann und nur dann kubischer Rest* (*mod.* p), *wenn in* (1) x *oder* y *durch* 5 *teilbar ist.*

7 *ist dann und nur dann kubischer Rest* (*mod.* p), *wenn in* (1) x *oder* y *durch* 7 *teilbar ist.*

2. **I. Kriterium:** *Ist* $p = 1 + 2^{2n} \cdot 3^{2m+3}$ *eine Primzahl* ($n > 0, m \geqq 0$), *so ist* 5 *dann und nur dann primitive Wurzel von* p, *wenn* n *und* m *gleiche Parität haben.*

Beweis: Es sind nur die Lösungen von

$$5 \equiv u^2 \quad \text{und} \quad 5 \equiv v^3 \quad (\text{mod. } p)$$

zu untersuchen. Haben diese keine Lösungen, so ist 5 primitive Wurzel (mod. p). Nun ist wegen $3 \equiv 2^3$ (mod. 5):

$$p \equiv 1 + 2^{2n+6m+9} \ (\text{mod. } 5);$$

also ist wegen $2n + 6m + 9 \equiv 2(n + m) + 1$ (mod. 4) bei gleicher Parität von n und m : $2(n + m) + 1 \equiv 1$ (mod. 4) und

$$p \equiv 3 \ (\text{mod. } 5) \ ,$$

d. h.

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1.$$

Die erste Kongruenz hat keine Lösung. Haben n und m ungleiche Parität, so ist $2(n + m) + 1 \equiv 3$ (mod. 4) und

$$p \equiv 4 \ (\text{mod. } 5) \ ,$$

d. h.

$$\left(\frac{5}{p}\right) = +1.$$

5 ist quadratischer Rest (mod. p), also sicherlich keine primitive Wurzel von p.

Die zweite Kongruenz hat keine Lösung, da in der Darstellung (1) von p $x = 2$, $y = 2 \cdot 2^n \cdot 3^m$, also wegen 1. 5 kubischer Nichtrest ist, da x und y zu 5 teilerfremd sind.

Beispiel: Die einzige Primzahl p unter 10000 der verlangten Form, für die 5 primitive Wurzel ist, ist

$$n = 2 \ , \quad m = 0 \ , \quad p = 433 \ .$$

II. Kriterium: *Ist* $p = 1 + 2^{2n} \cdot 3^{2m+3}$ $(n > 0 \ , \ m \geqq 0)$ *eine Primzahl, so ist 7 dann und nur dann primitive Wurzel (mod. p), wenn* $2n+m \equiv 1$ *(mod. 3) ist.*

Beweis: Es ist wegen $2 \equiv 3^2$ (mod. 7):

$$p \equiv 1 + 3^{4n+2m+3} \equiv 1 - 3^{2(2n+m)} \pmod{7} \ .$$

$2n+m$ kann nicht durch 3 teilbar sein, weil sonst p durch 7 teilbar wäre gegen die Annahme, p sei Primzahl. Ist $2n + m \equiv 1$ (mod. 3), so folgt:

$$p \equiv 1 - 3^2 \equiv -1 \pmod{7} \ .$$

p ist quadratischer Nichtrest (mod. 7) und

$$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1 .$$

7 ist Nichtrest (mod. p); also hat

$$7 \equiv u^2 \pmod{p}$$

keine Lösung. Ist dagegen $2n + m \equiv 2$ (mod. 3), so wird

$$p \equiv 1 - 3^4 \equiv 1 - 4 \equiv 4 \pmod{7} \quad \text{und} \quad \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = +1 .$$

7 ist quadratischer Rest (mod. p), kann also nicht primitive Wurzel (mod. p) sein.

Anderseits ist 7 kubischer Nichtrest (mod. p), da in der Darstellung (1) von $p: x = 2$, $y = 2 \cdot 2^n \cdot 3^m$ ist, also beide zu 7 teilerfremd sind, was nach 1. unsere Behauptung rechtfertigt.

Beispiel: Die einzige Primzahl unter 10000, für die 7 primitive Wurzel ist, und die die gewünschte Form hat, ist:

$$n = 2 \ , \quad m = 0 \ , \quad p = 433 \ .$$

3. III. Kriterium: *Ist $p = 1 + 3 \cdot 4\, q$ eine Primzahl, wo q selbst Primzahl ist, so ist 2 dann und nur dann primitive Wurzel von p, wenn m in der Darstellung $p = n^2 + 3\, m^2$ zu 3 teilerfremd ist.*

Beweis: Es ist für die gemachte Annahme die Unmöglichkeit der Kongruenzen:

$$2 \equiv u^2, \quad 2 \equiv v^3, \quad 2 \equiv w^q \quad (\text{mod. } p)$$

nachzuweisen. q ist jedenfalls nicht $= 2$. Daher muß q ungerade sein; also wird:

$$p \equiv 5 \quad (\text{mod. } 8) \ .$$

2 ist quadratischer Nichtrest von p.

Andererseits ist p stets darstellbar in der Form:

$$p = n^2 + 3\, m^2 \ . \quad n, \ m \text{ natürliche Zahlen} \ .$$

Nach 1. ist 2 nur kubischer Rest (mod. p), wenn m durch 3 teilbar ist, da ja von den drei Darstellungen (1) und (2) *nur eine* gerade Basen der Quadrate besitzt.

Es ist noch die dritte mögliche Kongruenz:

$$2 \equiv w^q \ (\text{mod. } p)$$

zu betrachten. Aus ihr folgt:

$$2^{12} \equiv 1 \ (\text{mod. } p) \ , \quad \text{oder} \quad 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13 \equiv 0 \ (\text{mod. } p).$$

p kann nur $= 13$ sein, was $n = 1$, $m = 2$, $q = 1$ verlangt. 2 ist aber primitive Wurzel von $p = 13$.

Beispiele von Primzahlen p, für die 2 primitive Wurzel ist:

n	m	q	p
1	2	1	13
5	2	3	37
7	2	5	61
7	10	29	349
19	2	31	373
11	14	59	709
29	2	71	853
17	14	73	877

IV. Kriterium: *Ist* $p = 1 + 2 \cdot 3q \neq 13$ *eine Primzahl, wo* q *selbst Primzahl ist, und ist:*

$$4p = n^2 + 27m^2, \qquad n, m \text{ natürliche Zahlen},$$

so ist 3 *dann und nur dann primitive Wurzel* (*mod.* p), *wenn* m *zu* 3 *teilerfremd ist.*

5, *resp.* 7 *sind dann und nur dann primitive Wurzeln* (*mod.* p), *wenn:*

$$n \equiv \pm m \not\equiv 0 \pmod{5}, \text{ resp. } n \equiv \pm 3m \not\equiv 0 \pmod{7},$$

ist, wo für 7 $p = 43$ *auszuschließen ist.*

Beweis: q kann nicht $= 2$ sein. Daher hat p die Form $12N + 7$, und es ist:

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1.$$

3 ist somit quadratischer Nichtrest (mod. p). Wegen

$$4p = n^2 + 27m^2$$

ist nach 1. 3 dann und nur dann kubischer Rest (mod. p), wenn m

durch 3 teilbar ist. Schließlich könnte noch

$$3 \equiv w^q \pmod{p}$$

sein, woraus aber:

$$3^6 \equiv 1 \pmod{p} \quad \text{oder} \quad 728 = 2^3 \cdot 7 \cdot 13 \equiv 0 \pmod{p}$$

folgte. Für 7 ist $q = 1$, und 13 ist ausgeschlossen.

Um den zweiten Teil des Satzes zu beweisen, bedenken wir, daß 5 niemals primitive Wurzel (mod. p) ist, wenn n oder m durch 5 teilbar ist, da dann nach 1. 5 kubischer Rest (mod. p) ist. Daher sind nur die beiden Fälle:

$$n \equiv \pm m \not\equiv 0 \quad \text{oder} \quad n \equiv \pm 2m \not\equiv 0 \pmod{5}$$

zu untersuchen. Im ersten Fall ist:

$$4p \equiv 3m^2 \pmod{5} ,$$

und:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = -1 .$$

Im zweiten Fall ist:

$$4p \equiv m^2 \pmod{5} \quad \text{und} \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 ,$$

d. h. 5 kann nicht primitive Wurzel sein. Schließlich folgt aus $5 \equiv w^q$ (mod. p):

$$5^6 - 1 = 2^3 \cdot 3^2 \cdot 7 \cdot 31 \equiv 0 \pmod{p} ,$$

was für $p = 31$ eine Darstellung ergibt, für die (siehe die nächste Tabelle) $n \not\equiv \pm m$ (mod. 5) wird, und 5 ist nicht primitive Wurzel. Die Behauptung ist in allen Fällen bewiesen.

Der Beweis für die Zahl 7 ist entsprechend. Da wieder nach 1. n und m zu 7 teilerfremd sein müssen, damit 7 kubischer Nichtrest ist, so sind die Fälle:

$$n \equiv \pm m \not\equiv 0 , \quad n \equiv \pm 2m \not\equiv 0 , \quad n \equiv \pm 3m \not\equiv 0 \pmod{7} ,$$

zu untersuchen. Im ersten ist $p \equiv 0$ (mod. 7), was unmöglich ist. Im zweiten ist: $4p \equiv 3m^2$ (mod. 7), und:

$$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = 1\,,$$

also 7 quadratischer Rest und somit keine primitive Wurzel (mod. p). Im dritten Fall ist: $4p \equiv m^2$ (mod. 7), also:

$$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = -\left(\frac{1}{7}\right) = -1\,.$$

7 ist quadratischer Nichtrest (mod. p). Ist schließlich $7 \equiv w^q$ (mod. p), so muß:

$$7^6 - 1 = 2^4 \cdot 3^2 \cdot 19 \cdot 43 \equiv 0 \pmod{p}$$

sein, was nur für $p = 43 = 4^2 + 27 \,.\, 1^2$ eine Darstellung in der verlangten Form mit $8 \equiv -3 \,.\, 2$ (und 7) zuläßt. Dieser Fall muß daher ausgeschlossen werden, und die Behauptung ist in allen Fällen bewiesen.

Beispiele:

n	m	q	p	*primitive Wurzeln*
7	1	3	19	3
2 . 2	2 . 1	5	31	3
2 . 4	2 . 1	7	43	3,5
5	3	11	67	7
17	1	13	79	3,7
13	3	17	103	5
23	1	23	139	3
2 . 14	2 . 1	37	223	3,5
2 . 16	2 . 1	47	283	3,5
2 . 16	2 . 3	83	499	7
2 . 16	2 . 7	263	1579	3

Bei diesen und den frühern Kriterien erhebt sich die interessante Frage, ob es unendlich viele Primzahlen der verlangten Form gibt.

(Eingegangen den 18. Dezember 1945.)