Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0140
LOG Titel: V. Theorie der Potenzreste für zusammengesetzte Moduli.
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

V. Theorie der Potenzreste für zusammengesetzte Moduli.

§. 127.

Es ist in §. 28 gezeigt, dass wenn die Zahl a relative Primzahl gegen den Modul k ist, stets positive ganze Exponenten n von der Beschaffenheit existiren, dass $a^n \equiv 1 \pmod{k}$ ist; diese Exponenten n sind die sämmtlichen Vielfachen des kleinsten unter ihnen; bezeichnet man diesen mit δ, so sagt man, die Zahl a *gehöre* zum Exponenten δ; und die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

sind sämmtlich incongruent. Mit Hülfe des verallgemeinerten Fermat'schen Satzes ist dort ebenfalls gezeigt, dass δ immer ein Divisor von $\varphi(k)$ ist; dies Resultat lässt sich aber auch ohne Hülfe des Fermat'schen Satzes ableiten durch eine eigenthümliche Methode, welche sehr häufig zum Nachweise der Theilbarkeit einer Zahl durch eine andere gebraucht werden kann. In unserm Falle gestaltet dieselbe sich folgendermaassen.

Ist a' irgend eine relative Primzahl zu k, so sind (nach §. 18) die δ Zahlen

$$a',\ a'a,\ a'a^2 \ldots a'a^{\delta-1} \qquad (A')$$

sämmtlich incongruent; dasselbe gilt von den δ Zahlen

$$a'',\ a''a,\ a''a^2 \ldots a''a^{\delta-1} \qquad (A'')$$

sobald a'' ebenfalls relative Primzahl zu k ist. Jeder solche Complex, wie A' oder A'', enthält δ unter einander incongruente Zahlen, die sämmtlich relative Primzahlen gegen k sind und also als

Repräsentanten von δ Zahl-Classen in Bezug auf den Modul k angesehen werden können. Gesetzt nun, es findet sich eine und dieselbe Zahlclasse in jedem der beiden Complexe A' und A'' vertreten, so giebt es zwei Exponenten μ', μ'' von der Beschaffenheit, dass

$$a' \cdot a^{\mu'} \equiv a'' \cdot a^{\mu''} \pmod{k}$$

ist; nehmen wir an, was der Symmetrie wegen erlaubt ist, dass $\mu'' \geqq \mu'$, so erhält man durch Division mit $a^{\mu'}$ die Congruenz

$$a' \equiv a'' \cdot a^{\mu''-\mu'} \pmod{k};$$

und hieraus folgt sogleich, dass *jede* in A' enthaltene Zahl $a' \cdot a^m$ auch einer Zahl von der Form $a'' \cdot a^n$, d. h. einer in A'' enthaltenen Zahl congruent ist. Wir können hieraus schliessen, dass entweder zwei solche Complexe A', A'' dieselben δ Zahlclassen enthalten, oder dass keine einzige Classe in beiden gleichzeitig vertreten ist.

Bildet man nun der Reihe nach alle solche aus δ Zahlclassen bestehenden Complexe von der Form A', A'' . . ., und zwar nur solche, welche von einander verschieden sind, so muss endlich jede der $\varphi(k)$ Zahlclassen, welche relative Primzahlen zu k enthalten, in einem dieser Complexe, und auch nur in einem, vertreten sein; ist daher ε die Anzahl dieser von einander verschiedenen Complexe, so muss $\varphi(k) = \varepsilon\delta$, also $\varphi(k)$ theilbar durch δ sein, was zu beweisen war.

Hieraus ergiebt sich nun der Fermat'sche Satz als Folgerung; denn erhebt man die Congruenz

$$a^{\delta} \equiv 1 \pmod{k}$$

zur εten Potenz, so erhält man

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

§. 128.

Für den Fall, dass der Modul k eine Primzahl p ist, wurde ferner in §. 29 bewiesen, dass zu jedem Divisor δ von $\varphi(p) = p-1$ genau $\varphi(\delta)$ Zahlen gehören, die nach dem Modul p incongruent sind; und in §. 30 sind die Eigenschaften der sogenannten primi-

tiven Wurzeln von p betrachtet, d. h. derjenigen $\varphi(p-1)$ incongruenten Zahlen g, welche zum Exponenten $p-1$ selbst gehören. Wir wollen nun untersuchen, ob ähnliche Gesetze auch für zusammengesetzte Moduln gelten.

Zunächst beschränken wir uns auf den Fall, in welchem der Modul k eine *Potenz von einer ungeraden Primzahl* p ist, und wir werden der Analogie nach unter einer *primitiven Wurzel* von k jede Zahl g verstehen, welche zum Exponenten $\varphi(k)$ gehört. Dem Beweise der wirklichen Existenz solcher primitiven Wurzeln schicken wir folgenden Hülfssatz voraus:

Ist h irgend eine ganze Zahl und $\pi \geqq 1$ eine positive ganze Zahl, so ist stets

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}.$$

Man überzeugt sich hiervon leicht durch die Entwicklung der linken Seite nach dem binomischen Satze; man findet nämlich zunächst, indem man sich auf die drei ersten Glieder beschränkt,

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} + \tfrac{1}{2}(p-1)h^2p^{2\pi+1} \pmod{p^{3\pi}},$$

und hieraus ergiebt sich die obige Congruenz, wenn man bedenkt, dass p ungerade, also $\frac{1}{2}(p-1)$ eine ganze Zahl, und ferner, dass sowohl $p^{2\pi+1}$ als auch $p^{3\pi}$ durch $p^{\pi+2}$ theilbar ist.

Nach dieser Vorbemerkung gehen wir an unsere Untersuchung und nehmen zunächst einmal an, es existire für den Modul $p^{\pi+1}$, wo $\pi \geqq 1$ ist, wirklich eine primitive Wurzel g; dann liegt es nahe zu fragen: zu welchem Exponenten gehört eine solche Zahl g in Bezug auf den Modul p^{π}? Es sei δ dieser Exponent, also

$$g^{\delta} = 1 + hp^{\pi},$$

so erhält man mit Hülfe des soeben bewiesenen Satzes

$$g^{\delta p} \equiv 1 \pmod{p^{\pi+1}};$$

da nun g primitive Wurzel von $p^{\pi+1}$ ist, so muss δp durch $\varphi(p^{\pi+1}) = (p-1)p^{\pi}$, und folglich δ durch $(p-1)\,p^{\pi-1}$ theilbar sein; andererseits muss aber, da g zum Exponenten δ in Bezug auf den Modul p^{π} gehört, nothwendig $\varphi(p^{\pi}) = (p-1)\,p^{\pi-1}$ durch δ theilbar sein; mithin ist $\delta = \varphi(p^{\pi})$, d. h. g ist auch primitive Wurzel von p^{π}. Zugleich leuchtet ein, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^{\pi}$$

vorkommende Zahl h nicht durch p theilbar sein kann; denn sonst wäre

$$g^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^{\pi+1}},$$

also g keine primitive Wurzel von $p^{\pi+1}$.

Setzt man diese Schlüsse weiter fort, so erhält man zunächst das Resultat:

Jede primitive Wurzel g von einer höhern Potenz einer ungeraden Primzahl p ist nothwendig eine primitive Wurzel der Zahl p selbst, und zwar von der Beschaffenheit, dass $g^{p-1} - 1$ nicht durch p^2 theilbar ist.

Wir wollen nun umgekehrt annehmen, es sei g eine primitive Wurzel von p^π, und zwar von der Beschaffenheit, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar ist; und wir fragen jetzt: zu welchem Exponenten gehört diese Zahl g in Bezug auf den Modul $p^{\pi+1}$? Ist δ dieser Exponent, also

$$g^\delta \equiv 1 \pmod{p^{\pi+1}},$$

so ist auch

$$g^\delta \equiv 1 \pmod{p^\pi},$$

und folglich δ theilbar durch $\varphi(p^\pi)$; da aber andererseits δ ein Divisor von $\varphi(p^{\pi+1}) = p\varphi(p^\pi)$ sein muss, so ist δ entweder $= \varphi(p^\pi)$, oder $= \varphi(p^{\pi+1})$; das Erstere ist aber nicht der Fall, weil unserer Voraussetzung zufolge die Zahl h nicht durch p theilbar ist; also ist $\delta = \varphi(p^{\pi+1})$, d. h. die Zahl g ist primitive Wurzel von $p^{\pi+1}$. Zugleich leuchtet aus der Congruenz

$$g^{(p-1)p^\pi} = (1 + hp^\pi)^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}$$

ein, dass die in der Gleichung

$$g^{(p-1)p^\pi} = 1 + h'p^{\pi+1}$$

vorkommende Zahl h' nicht durch p theilbar ist.

Durch Fortsetzung dieser Schlussweise erhalten wir das zweite Resultat:

Jede primitive Wurzel g einer ungeraden Primzahl p, für welche die Differenz $g^{p-1} - 1$ nicht durch p^2 theilbar ist, ist auch eine primitive Wurzel aller höheren Potenzen von p.

Um also die Existenz von primitiven Wurzeln g für höhere Potenzen von p nachzuweisen, und um alle diese Zahlen g zu finden, haben wir nur noch zu zeigen, dass in der That primitive Wurzeln g von p existiren, für welche $g^{p-1} - 1$, oder, was dasselbe sagt, für welche $g^p - g$ nicht durch p^2 theilbar ist. Dies geschieht leicht auf folgende Weise. Ist f irgend eine primitive Wurzel von p, so sind alle in der Form

$$g = f + px$$

enthaltenen Zahlen g ebenfalls primitive Wurzeln von p; dann ist nach dem binomischen Satze

$$g^p \equiv f^p \pmod{p^2};$$

setzen wir daher

$$f^p \equiv f + f'p \pmod{p^2},$$

so wird

$$g^p - g \equiv p(f' - x) \pmod{p^2},$$

und folglich ist $g = f + px$ jedesmal eine primitive Wurzel aller Potenzen von p, ausgenommen, wenn $x \equiv f' \pmod{p}$, also

$$g \equiv f^p \pmod{p^2}$$

ist. Da nun $\varphi(p-1)$ nach dem Modul p incongruente Zahlen f existiren, und aus jeder Zahl f genau $(p-1)$ in Bezug auf den Modul p^2 incongruente Zahlen $g = f + px$ von der Beschaffenheit abgeleitet werden können, dass $g^{p-1} - 1$ nicht durch p^2 theilbar wird, so erhalten wir das Resultat:

Die sämmtlichen primitiven Wurzeln von höheren Potenzen einer ungeraden Primzahl p sind die sämmtlichen Individuen von $(p-1)\,\varphi(p-1)$ verschiedenen Zahlclassen in Bezug auf den Modul p^2.

Beispiel: Sämmtliche primitive Wurzeln der Primzahl $p = 7$ sind in den beiden Reihen $7x + 3$, $7x + 5$ enthalten; da nun

$$3^7 \equiv 31, \quad 5^7 \equiv 19 \pmod{49}$$

ist, so sind alle in den arithmetischen Reihen $7x + 3$, $7x + 5$ enthaltenen Zahlen, mit Ausnahme derer, welche $\equiv 31$ oder $\equiv 19 \pmod{49}$ sind, auch primitive Wurzeln von allen höheren Potenzen von 7.

§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0,\ g^1,\ g^2 \ldots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschluss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ, die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl n für die Basis g*, und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c, so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. } (1) \equiv 0,\quad \text{Ind. } (-1) \equiv \tfrac{1}{2}c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind.}n} \pmod{p^\pi}$$

folgt nämlich

$$n^t \equiv g^{t\,\mathrm{Ind}.n} \pmod{p^\pi};$$

soll also $n^t \equiv 1$ sein, so muss t Ind. n durch c theilbar, und folglich t ein Multiplum von $c : \delta$ sein, wo δ den grössten gemeinschaftlichen Divisor von c und Ind. n bedeutet; die kleinste aller dieser Zahlen t, d. h. der Exponent, zu welchem n gehört, ist daher $= c : \delta$.

Hieraus folgt, dass n stets und nur dann eine primitive Wurzel von p^π ist, wenn Ind. n relative Primzahl zu c ist; die Anzahl aller nach dem Modul p^π incongruenten primitiven Wurzeln von p^π ist daher gleich der Anzahl derjenigen der Zahlen

$$0,\ 1,\ 2 \ldots c-1,$$

welche relative Primzahlen zu c sind, also gleich $\varphi(c) = \varphi\varphi(p^\pi)$. Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlusssatze des vorigen Paragraphen.

§. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul $2^2 = 4$ ist $3 \equiv -1$ eine primitive Wurzel; zu jeder ungeraden Zahl n giebt es einen entsprechenden Exponenten α von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist $\alpha \equiv 0 \pmod{2}$ oder $\equiv 1 \pmod{2}$, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul 2^λ betrachtet wird, in welchem der Exponent $\lambda \geqq 3$ ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn n irgend eine ungerade Zahl bedeutet, immer schon

$$n^{\frac{1}{2}\varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für $\lambda = 3$; denn das Quadrat jeder ungeraden Zahl n ist $\equiv 1 \pmod{8}$. Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten $\lambda \geqq 3$ schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h\,2^{\lambda},$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h\,2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten $\lambda + 1$. Er gilt mithin allgemein, da er für $\lambda = 3$ gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$ gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul $2^{\lambda} \geqq 8$ besitzt. Es ist nämlich

$$5 \equiv 1 + 4 \pmod{8}$$
$$5^2 \equiv 1 + 8 \pmod{16}$$
$$5^4 \equiv 1 + 16 \pmod{32}$$
$$5^8 \equiv 1 + 32 \pmod{64}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}},$$

also

$$5^{2^{\lambda-3}} \text{ niemals} \equiv 1 \pmod{2^{\lambda}},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul 2^{λ} gehört, kein Divisor von $2^{\lambda-3}$ sein kann, und also, da er doch Divisor von $2^{\lambda-2}$ sein muss, nothwendig $= 2^{\lambda-2}$ ist.

Hieraus ergiebt sich nun, wenn man zur Abkürzung

$$\tfrac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} = b$$

setzt, dass die b Zahlen

$$5^0,\ 5^1,\ 5^2 \ldots 5^{b-1}$$

sämmtlich nach dem Modul 2^{λ} incongruent sind; dasselbe gilt von den Zahlen

$$-5^0,\ -5^1,\ -5^2 \ldots -5^{b-1}$$

da ferner die erstern sämmtlich $\equiv 1 \pmod 4$, die letztern sämmtlich $\equiv 3 \pmod 4$ sind, so bilden sie zusammengenommen ein System von $\varphi(2^{\lambda})$ nach dem Modul 2^{λ} incongruenten ungeraden Zahlen. Ist daher n irgend eine ungerade Zahl, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

setzen, wo α nach dem Modul 2, und β nach dem Modul b vollständig bestimmt ist. Durchläuft α ein vollständiges Restsystem in Bezug auf den Modul 2, und β unabhängig von α ein vollständiges Restsystem in Bezug auf den Modul b, so durchläuft n ein vollständiges System von Zahlen, die in Bezug auf den Modul 2^{λ} incongruent und relative Primzahlen zu 2^{λ}, d. h. ungerade sind. Diese beiden Zahlen α und β kann man die *Indices* der Zahl n nennen; sie befolgen ganz ähnliche Gesetze, wie die Indices für die früher betrachteten Moduli. Wir heben noch besonders hervor, dass $n \equiv \pm 1$ oder $\equiv \pm 3 \pmod{8}$ ist, je nachdem β gerade oder ungerade.

Es verdient bemerkt zu werden, dass die vorstehende Form, in welche jede ungerade Zahl n gebracht werden kann, auch noch für den Fall $\lambda = 2$ gilt; die Anzahl b der Werthe von β reducirt sich nämlich auf 1, und da $5 \equiv 1 \pmod{4}$, so geht die obige Form in die frühere $n \equiv (-1)^{\alpha} \pmod{4}$ über. Für eine spätere Untersuchung ist es sogar zweckmässig, dieselbe Form der Darstellung aller relativen Primzahlen zu einem Modul von der Form 2^{λ} auf die Fälle $\lambda = 0$ und $\lambda = 1$ auszudehnen; da in denselben nur eine einzige Zahlclasse darzustellen ist, so wird man α und β auch nur einen einzigen Werth beizulegen haben; setzen wir daher $a = b = 1$, wenn $\lambda = 0$ oder $\lambda = 1$ ist, in allen anderen Fällen ($\lambda \geqq 2$) aber $a = 2$, $b = \frac{1}{2}\varphi(2^{\lambda})$, so können wir sagen, dass der Ausdruck

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

alle incongruenten relativen Primzahlen zum Modul durchläuft, wenn α und β resp. vollständige Restsysteme in Bezug auf a und b durchlaufen.

§. 131.

Es sei nun der Modul eine beliebige zusammengesetzte Zahl

$$k = 2^{\lambda} p^{\pi} p'^{\pi'} \ldots,$$

wo p, p' von einander verschiedene ungerade Primzahlen, und λ, π, π' . . . ganze positive Exponenten bedeuten, deren erster, λ,

auch $= 0$ sein kann. Ist n irgend eine relative Primzahl zu k, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$
$$n \equiv g^{\gamma} \pmod{p^{\pi}}$$
$$n \equiv g'^{\gamma'} \pmod{p'^{\pi'}}$$
$$\ldots\ldots\ldots\ldots$$

setzen, wo $g, g' \ldots$ primitive Wurzeln resp. von $p^2, p'^2 \ldots$ bedeuten. Geben wir den Zahlen a, b die im vorigen Paragraphen festgesetzte Bedeutung und setzen wir zur Abkürzung

$$\varphi(p^{\pi}) = c, \quad \varphi(p'^{\pi'}) = c' \ldots,$$

so sind die Exponenten oder Indices

$$\alpha, \ \beta, \ \gamma, \ \gamma' \ldots$$

vollständig bestimmt in Bezug auf die entsprechenden Moduli

$$a, \ b, \ c, \ c' \ldots,$$

und umgekehrt entspricht jedem solchen Systeme von Indices (nach §. 25) eine bestimmte Classe von Zahlen n nach dem Modul k, die relative Primzahlen zu k sind. Durchlaufen die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ unabhängig von einander ihre $a, b, c, c' \ldots$ Werthe, so durchläuft n sämmtliche

$$abcc' \ldots = \varphi(k)$$

Zahlclassen in Bezug auf den Modul k, welche relative Primzahlen zu k enthalten.

Sind die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ einer Zahl n bekannt, so ist es leicht, den Exponenten δ zu bestimmen, zu welchem die Zahl n gehört; denn offenbar ist δ das kleinste gemeinschaftliche Multiplum aller derjenigen Exponenten, zu welchen die Zahl n in Bezug auf die einzelnen Moduli $2^{\lambda}, p^{\pi}, p'^{\pi'} \ldots$ gehört. Dieser Exponent δ ist daher immer ein Divisor von dem kleinsten gemeinschaftlichen Vielfachen μ der Zahlen $a, b, c, c' \ldots$ Es können daher primitive Wurzeln von k, d. h. Zahlen, die zum Exponenten $\varphi(k)$ gehören, nur dann existiren, wenn $\mu = \varphi(k)$ ist; man überzeugt sich leicht, dass dies nur dann der Fall ist, wenn der Modul $k = 1$, oder $= 2$, oder $= 4$, oder eine Potenz einer ungeraden Primzahl, oder das Doppelte einer solchen Potenz ist; und umgekehrt leuchtet ein, dass in diesen Fällen immer primitive Wurzeln existiren.

Da ferner die Möglichkeit einer binomischen Congruenz von der Form

$$x^m \equiv n \pmod{k}$$

und die Anzahl ihrer Wurzeln nur von der Möglichkeit derselben Congruenz in Bezug auf die einzelnen Moduli 2^λ, p^π, $p'^{\pi'}$ ... abhängt (nach §. 37), so überzeugt man sich leicht, dass zur Beurtheilung dieser Frage und zur Auffindung der Wurzeln der Congruenz die Kenntniss der Indices der Zahl n vollständig ausreicht. Die wirkliche Ausführung dieser Untersuchung unterdrücken wir hier, weil sie sich ganz ebenso gestaltet wie in §. 31. Der Fall $m = 2$ würde auf diese Weise behandelt auf das in §. 37 gewonnene Resultat zurückführen. Ebenso leicht ist es, den verallgemeinerten Wilson'schen Satz (§. 38) von Neuem zu beweisen.