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_0023
LOG Titel: Zweiter Abschnitt: Von der Congruenz der Zahlen.
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

Zweiter Abschnitt.

Von der Congruenz der Zahlen.

§. 17.

Bedeutet k irgend eine positive ganze Zahl, so lässt sich jede beliebige ganze Zahl a stets und nur auf eine einzige Weise in die Form

$$a = sk + r$$

bringen, in welcher s eine ganze Zahl und r eine der k Zahlen

$$0, 1, 2 \ldots (k-1)$$

bedeutet. Denn lässt man zunächst s alle ganzen Zahlwerthe von $-\infty$ bis $+\infty$ durchlaufen, so bilden die Zahlen sk die sämmtlichen Multipla von k, und von einem solchen Multiplum sk bis zum nächst grössern $(s+1)k$ excl. giebt es immer nur k Zahlen, nämlich

$$sk, sk+1, sk+2 \ldots sk+(k-1);$$

giebt man daher dem s alle denkbaren ganzen Zahlwerthe, und dem r jedesmal alle jene bestimmten k Werthe, so durchläuft der Ausdruck $sk+r$ wirklich alle ganzen Zahlwerthe a; dass ferner jede Zahl a auf diese Weise nur ein einziges Mal erzeugt wird, leuchtet auf folgende Weise ein. Wenn

$$s'k + r' = sk + r$$

ist, so folgt daraus

$$r' - r = (s - s')k;$$

wenn nun r' ebenfalls eine der k Zahlen $0, 1, 2 \ldots (k-1)$ ist, so ist der absolute Werth von $r'-r$ ebenfalls eine dieser Zahlen, also kleiner als k; da aber $r'-r$ ein Multiplum von k ist, so kann $r'-r$ nur $= 0$ sein, woraus $r' = r$ und $s' = s$ folgt.

Wir werden nun im Folgenden sagen, dass die Zahl r der *Rest* der Zahl a in Bezug auf den *Modulus* k ist; sobald ferner zwei Zahlen a und b in Bezug auf denselben Modulus k denselben Rest r lassen, sollen sie *gleichrestig* oder (nach *Gauss*) *congruent* in Bezug auf den Modulus k heissen; da in diesem Fall $a = sk+r$ und $b = s'k+r$ ist, so folgt, dass die Differenz $a-b = (s-s')k$ durch den Modulus k theilbar ist; und umgekehrt, ist $a-b$ durch k theilbar, so sind die Zahlen a und b auch congruent in Bezug auf den Modul k; denn ist r der Rest von a, r' der von b, also

$$a = sk+r, \quad b = s'k+r',$$

so ist

$$a-b = (s-s')k+(r-r');$$

da nun der Voraussetzung nach $a-b$ ein Multiplum von k ist, so muss auch $r'-r$ ein solches sein, was, wie wir vorher gesehen haben, nicht anders möglich ist, als wenn $r' = r$ ist. Man könnte daher congruente Zahlen auch als solche definiren, deren Differenz durch den Modul theilbar ist. (Aus diesem Grunde hat man die Bedeutung des Wortes Rest in der Weise erweitert, dass jede von zwei einander nach dem Modul k congruenten Zahlen a und b ein *Rest* der andern heisst.)

Da man sehr häufig die Congruenz zweier Zahlen a und b in Bezug auf eine dritte k als Modul auszudrücken hat, so ist von *Gauss**) für dieselbe folgende Bezeichnung eingeführt:

$$a \equiv b \pmod{k}.$$

So ist z. B.

$$3 \equiv -25 \pmod{4}, \quad 65 \equiv 16 \pmod{7}.$$

Da die beiden Zahlen a und b in dem Begriffe der Congruenz dieselbe Rolle spielen, so darf man offenbar die zur Linken und Rechten des Zeichens $\equiv$ stehenden Zahlen mit einander vertauschen. Ferner leuchten aus dem Begriffe der Congruenz leicht die folgenden Sätze ein:

1. Sind a und k zwei beliebige Zahlen, so ist stets

$$a \equiv a \pmod{k}.$$

*) *D. A.* art. 2.

2. Ist in Bezug auf denselben Modulus k eine erste Zahl a einer zweiten b, diese wieder einer dritten c congruent, so ist auch die erste a der dritten c in Bezug auf k congruent; in Zeichen: ist

$$a \equiv b \pmod{k}, \quad b \equiv c \pmod{k},$$

so ist auch

$$a \equiv c \pmod{k}.$$

Denn die Reste der drei Zahlen a, b, c sind einander gleich; oder auch, da $a-b$ und $b-c$ Multipla von k sind, so ist auch $(a-b)+(b-c)=a-c$ Multiplum von k.

3. Ist

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$a+m \equiv b+n \pmod{k} \text{ und } a-m \equiv b-n \pmod{k}.$$

Denn da $a-b$ und $m-n$ Multipla von k sind, so sind auch $(a-b)+(m-n)=(a+m)-(b+n)$ und $(a-b)-(m-n)=(a-m)-(b-n)$ Multipla von k.

Dies lässt sich für eine beliebige Anzahl von Congruenzen erweitern, die sich auf denselben Modulus beziehen; man kann sie addiren und subtrahiren wie Gleichungen.

4. Ist wieder

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$am \equiv bn \pmod{k}.$$

Denn da $a-b$ ein Vielfaches von k ist, so ist zunächst auch $(a-b)\,m=am-bm$ ein solches, also

$$am \equiv bm \pmod{k};$$

da ferner $m-n$ ein Vielfaches von k ist, so ist auch $b(m-n)=bm-bn$ ein solches, also

$$bm \equiv bn \pmod{k};$$

die beiden Zahlen am und bn sind daher derselben Zahl bm congruent, folglich sind sie auch unter einander congruent.

Auch dieser Satz lässt sich dahin verallgemeinern, dass man eine ganze Reihe von Congruenzen, die sich auf denselben Modul beziehen, mit einander multipliciren kann wie Gleichungen; und hieraus folgt wieder, dass gleich hohe Potenzen zweier congruenten Zahlen wieder congruent sind in Bezug auf denselben Modulus.

5. Die bisherigen Sätze kann man folgendermaassen zusammenfassen. Ist $f(x, y, z \ldots)$ eine ganze rationale Function der

Unbestimmten $x, y, z \ldots$, deren Coefficienten ganze Zahlen sind, und ist in Bezug auf einen und denselben Modulus k

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

so ist auch

$$f(a,b,c \ldots) \equiv f(a',b',c' \ldots) \pmod{k}.$$

6. Etwas anders verhält es sich bei der Division. Ist nämlich

$$am \equiv bm \pmod{k},$$

so kann man hieraus im Allgemeinen nicht mit Sicherheit schliessen, dass auch $a \equiv b \pmod{k}$ sein muss; bezeichnen wir mit δ den grössten gemeinschaftlichen Divisor der beiden Zahlen $m = m'\delta$ und $k = k'\delta$, so folgt aus der obigen Congruenz nur, dass

$$a \equiv b \left(\mathrm{mod.}\frac{k}{\delta}\right)$$

sein muss. Denn da $m(a-b)$ durch k, also $m'(a-b)$ durch k' theilbar, und m' relative Primzahl gegen k' ist, so muss $(a-b)$ durch k' theilbar sein.

7. Ist

$$a \equiv b \pmod{k}$$

und m irgend ein Divisor von k, so ist auch

$$a \equiv b \pmod{m}.$$

Denn $a-b$ ist ein Multiplum von k, und k ein Multiplum von m; also ist $a-b$ auch ein Multiplum von m.

8. Ist

$a \equiv b \pmod{k}$ und $a \equiv b \pmod{l}$ und $a \equiv b \pmod{m}$ u. s. w., so ist auch

$$a \equiv b \pmod{h},$$

wo h das kleinste gemeinschaftliche Multiplum von $k, l, m \ldots$ bezeichnet. Denn $a-b$ ist ein gemeinschaftliches Multiplum aller dieser Zahlen, also auch Multiplum von h.

Hieraus folgt auch noch als ein besonders bemerkenswerther specieller Fall, dass, wenn eine Congruenz richtig ist in Bezug auf eine Reihe von Moduln, die sämmlich unter einander relative Primzahlen sind, dieselbe auch in Bezug auf einen Modul gilt, welcher das Product aus allen jenen Moduln ist.

Wir bemerken schliesslich, dass auch *negative* Moduln k zugelassen werden; das Zeichen $a \equiv b \pmod{k}$ bedeutet auch dann,

dass die Differenz $a - b$ durch k theilbar ist; offenbar behalten die vorstehenden Sätze auch nach dieser Erweiterung ihre volle Gültigkeit.

§. 18.

Da jede beliebige Zahl a ihrem Reste r in Bezug auf den (positiven) Modul k congruent ist, so ist jede Zahl a einer der k Zahlen

$$0, 1, 2 \ldots (k-1)$$

congruent; sie kann aber auch nur einer dieser Zahlen congruent sein, denn sonst müssten ja auch unter diesen k Resten mindestens zwei einander congruent sein, was offenbar nicht der Fall ist. Theilen wir daher sämmtliche Zahlen in *Classen* ein nach dem Princip, dass wir jedesmal zwei Zahlen in dieselbe oder in verschiedene Classen werfen, je nachdem sie in Bezug auf den Modulus k congruent sind oder nicht, so ist die *Anzahl* dieser Classen offenbar $= k$; die eine enthält sämmtliche Zahlen, welche $\equiv 0 \pmod{k}$, d. h. durch k theilbar sind; die folgende Classe enthält alle Zahlen, welche $\equiv 1 \pmod{k}$ sind, u. s. f.

Greift man nun aus jeder dieser Classen nach Belieben ein Individuum heraus, so hat das so gebildete System von k Zahlen die charakteristische Eigenschaft, dass jede beliebige ganze Zahl stets einer und auch nur einer von diesen k Zahlen congruent ist; ein solches System, wie es z. B. auch die Zahlen

$$0, 1, 2 \ldots (k-1)$$

bilden, nennt man ein *vollständiges System nicht congruenter* (oder *incongruenter*) *Zahlen* oder ein *vollständiges Restsystem* in Bezug auf den Modul k; offenbar bilden auch die Zahlen

$$1, 2, 3 \ldots k$$

und ebenso je k successive ganze Zahlen ein solches System.

Alle Zahlen, welche einer und derselben Classe angehören, haben nun mehrere allen gemeinschaftliche Eigenschaften, so dass sie in Bezug auf den Modul fast die Rolle einer einzigen Zahl spielen. Wir haben schon früher gesehen, dass jede Zahl, welche in einer Congruenz als Summand oder als Factor auftritt, unbeschadet der Richtigkeit der Congruenz durch jede andere ihr congruente, d. h. derselben Classe angehörige Zahl ersetzt werden

darf. Ein anderes Element, welches allen in einer Classe enthaltenen Individuen gemeinschaftlich ist, bildet der grösste Divisor, den sie mit dem Modul k gemeinschaftlich haben; denn sind a und b zwei congruente Zahlen, so ist

$$a = b + sk,$$

und folglich ist jeder gemeinschaftliche Divisor von a und k auch gemeinschaftlicher Divisor von b und k. Man kann daher nach diesem grössten gemeinschaftlichen Divisor die Classen wieder in Gruppen eintheilen, und da die Zahlen

$$1, 2 \ldots k$$

ein vollständiges System incongruenter Zahlen bilden, so ist (nach §. 13), wenn δ irgend einen Divisor von $k = n\delta$ bezeichnet, $\varphi(n)$ die Anzahl derjenigen Classen, welche solche Zahlen enthalten, die δ zum grössten gemeinschaftlichen Divisor mit dem Modul k haben. Speciell ist also $\varphi(k)$ die Anzahl derjenigen Classen, welche nur Zahlen enthalten, die relative Primzahlen gegen den Modulus k sind.

Von besonderer Wichtigkeit für spätere Untersuchungen ist auch noch folgender Satz:

Ist a relative Primzahl gegen den Modulus k, und setzt man in dem linearen Ausdruck $ax + b$ für x der Reihe nach alle k Glieder eines vollständigen Systems incongruenter Zahlen ein, so bilden die so entstehenden Werthe dieses Ausdrucks wieder ein vollständiges System incongruenter Zahlen.

Da nämlich aus

$$ax + b \equiv ay + b \pmod{k}$$

auch

$$ax \equiv ay \pmod{k}$$

und, da a relative Primzahl gegen k ist, nach §. 17, 6. auch

$$x \equiv y \pmod{k}$$

folgt, so ergiebt sich, dass alle Werthe des Ausdrucks $ax + b$, welche incongruenten Werthen von x entsprechen, ebenfalls incongruent sind; setzt man daher für x alle k incongruenten Zahlen ein, so erhält der Ausdruck $ax + b$ auch k incongruente Werthe, welche, da es überhaupt nur k Classen giebt, ein vollständiges System incongruenter Zahlen bilden.

§. 19.

Betrachten wir jetzt den Ausdruck ax, in welchem a wieder relative Primzahl gegen den Modul k ist, und setzen wir wieder für x der Reihe nach die Glieder eines vollständigen Systems incongruenter Zahlen ein, aber nicht alle, sondern nur diejenigen

$$a_1, a_2, a_3 \ldots,$$

welche relative Primzahlen gegen den Modul k sind, und deren Anzahl nach dem vorigen Paragraphen gleich $\varphi(k)$ ist, so leuchtet erstens ein, dass die Werthe des Ausdrucks ax, d. h. die Producte

$$aa_1, \quad aa_2, \quad aa_3 \ldots$$

sämmtlich incongruent sind, ferner, dass dieselben sämmtlich wieder relative Primzahlen gegen k sind; es wird daher jedes dieser Producte einem und nur einem Gliede der Reihe

$$a_1, a_2, a_3 \ldots$$

congruent sein. Wir können daher setzen

$$\left.\begin{aligned} aa_1 &\equiv b_1 \\ aa_2 &\equiv b_2 \\ aa_3 &\equiv b_3 \end{aligned}\right\} (\mathrm{mod.}\, k),$$

u. s. w.

wo nun die Zahlen

$$b_1, b_2, b_3 \ldots$$

vollständig, wenn auch in anderer Ordnung, mit den Zahlen

$$a_1, a_2, a_3 \ldots$$

übereinstimmen, so dass namentlich

$$a_1 a_2 a_3 \ldots a_{\varphi(k)} = b_1 b_2 b_3 \ldots b_{\varphi(k)}$$

sein wird. Bezeichnen wir zur Abkürzung dieses Product mit P, und multipliciren wir die vorstehenden $\varphi(k)$ Congruenzen mit einander, so erhalten wir daher

$$a^{\varphi(k)} \cdot P \equiv P \ (\mathrm{mod.}\, k).$$

Nun ist aber P ein Product von lauter Zahlen, die relative Primzahlen gegen den Modul sind, also selbst relative Primzahl gegen den Modul k; es ist daher nach §. 17, 6. gestattet, die vorstehende Congruenz durch den gemeinschaftlichen Factor P beider Seiten ohne Weiteres zu dividiren. Auf diese Weise erhalten wir die Congruenz

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

in Worten kann man diesen höchst wichtigen Satz folgendermaassen aussprechen:

Ist a relative Primzahl gegen die positive Zahl k, und erhebt man a zu einer Potenz, deren Exponent $\varphi(k)$ angiebt, wie viele der Zahlen

$$1, 2, 3 \ldots k$$

relative Primzahlen gegen k sind, so lässt diese Potenz, durch k dividirt, stets den Rest 1.

Nehmen wir z. B. $k = 15$, $a = 2$, so ist a wirklich relative Primzahl gegen k; nun ist $\varphi(k) = \varphi(15) = \varphi(3)\,\varphi(5) = 8$; es muss daher 2^8, durch 15 dividirt, den Rest 1 lassen; in der That ist

$$2^8 = 256 = 17 \cdot 15 + 1.$$

Es kann übrigens vorkommen, dass auch Potenzen von a mit niedrigerm Exponenten als $\varphi(k)$ denselben Rest 1 geben. Dies tritt wirklich in dem eben gewählten Beispiel ein, denn es ist auch

$$2^4 = 16 = 1 \cdot 15 + 1.$$

Specialisiren wir unsern Satz für den Fall, dass k nur durch eine einzige Primzahl p theilbar, also

$$k = p^\pi, \quad \varphi(k) = (p-1)p^{\pi-1}$$

ist, so erhalten wir den Satz:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^\pi}.$$

Nehmen wir ferner hierin $\pi = 1$, so erhalten wir einen berühmten Satz, der zuerst von *Fermat* aufgestellt ist und daher der Fermat'sche Satz heisst:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{p-1} \equiv 1 \pmod{p}.$$

Man kann diesen Satz so umformen, dass er auch für den Fall gültig bleibt, wenn a durch p theilbar ist; zu diesem Zweck braucht man nur die vorstehende Congruenz mit a zu multipliciren, wodurch sie in die folgende

$$a^p \equiv a \pmod{p}$$

übergeht. Ist nämlich a theilbar durch p, so sind beide Seiten dieser Congruenz $\equiv 0 \pmod{p}$, also ist sie auch dann noch richtig. Umgekehrt kann man aus dieser Form des Satzes auch wieder die

frühere ableiten; denn sobald a nicht theilbar durch p, also relative Primzahl gegen p ist, darf man beide Seiten dieser Congruenz auch wieder durch a dividiren, ohne den Modul zu ändern.

Kehren wir zu dem allgemeinen Satz zurück, der zuerst von *Euler**) bewiesen ist und den Namen des verallgemeinerten Fermat'schen Satzes führt, so können wir denselben auch in folgender Weise aussprechen: Sind p, r, s . . . von einander verschiedene absolute Primzahlen, und ist a durch keine dieser Primzahlen theilbar, so ist stets

$$a^{(p-1)p^{\pi-1}\cdot(r-1)r^{\varrho-1}\cdot(s-1)s^{\sigma-1}\cdots} \equiv 1 \pmod{p^\pi r^\varrho s^\sigma \ldots},$$

wo π, ϱ, σ . . . irgend welche ganze positive Zahlen bedeuten.

§. 20.

Es ist wohl nicht überflüssig, dem vorhergehenden Beweise dieses wichtigen Satzes einen zweiten hinzuzufügen, der gradatim zu Werke geht und sich zunächst auf den binomischen Satz stützt. Ist p irgend eine ganze positive Zahl, so ist zufolge dieses Satzes bekanntlich

$$(a+b)^p =$$

$$a^p + \frac{p}{1}a^{p-1}b + \cdots + \frac{p!}{r!(p-r)!}a^{p-r}b^r + \cdots + b^p;$$

hierin sind (nach §. 15) alle Coefficienten ganze Zahlen. Ist aber p eine Primzahl, so können wir hinzufügen, dass alle Coefficienten mit Ausnahme des ersten und letzten, welche $= 1$ sind, durch p theilbar sind; denn der Zähler des Bruches

$$\frac{p!}{r!(p-r)!},$$

in welchem r eine der Zahlen 1, 2, 3 . . . $(p-1)$ bedeutet, enthält den Factor p, der Nenner dagegen nicht; der Bruch ist also von der Form $pm:n$, wo n nicht theilbar durch p, also auch relative Primzahl gegen p ist; da wir aber ferner wissen, dass dieser Bruch eine ganze Zahl, dass also pm durch n theilbar ist, so muss m durch n theilbar sein; der Bruch hat daher die Form ps, wo der zweite Factor s eine ganze Zahl ist; und folglich ist jeder dieser $(p-1)$ Coefficienten $\equiv 0 \pmod{p}$. Sind daher a und b irgend welche ganze Zahlen, so erhalten wir die folgende Congruenz

$$(a+b)^p \equiv a^p + b^p \pmod{p},$$

*) *Theorematа arithm. nova meth. demonstr.*, Comm. nov. Ac. Petrop. VIII. p. 74.

wobei also vorausgesetzt ist, dass p eine Primzahl ist. Offenbar folgt hieraus weiter

$$(a+b+c)^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \pmod{p}$$

und allgemein für eine beliebige Reihe von n ganzen Zahlen a, $b \ldots h$:

$$(a+b+\cdots+h)^p \equiv a^p + b^p + \cdots + h^p \pmod{p}.$$

Setzen wir hierin $a = 1$, $b = 1 \ldots h = 1$, so erhalten wir für jede beliebige positive ganze Zahl n den Satz:

$$n^p \equiv n \pmod{p}.$$

Da ferner für jede ungerade Primzahl $(-1)^p \equiv -1$, und für die einzige gerade Primzahl $p = 2$ ebenfalls $(-1)^p = 1 \equiv -1 \pmod{p}$ ist, so erhalten wir durch Multiplication der vorstehenden Congruenz mit der andern

$$(-1)^p \equiv -1 \pmod{p}$$

die neue

$$(-n)^p \equiv -n \pmod{p}.$$

Also ist der Fermat'sche Satz

$$a^p \equiv a \pmod{p}$$

für jede positive und negative Zahl a bewiesen, während er für $a = 0$ unmittelbar evident ist. Wenn nun a nicht durch p theilbar ist, was wir von jetzt annehmen wollen, so folgt hieraus, dass

$$a^{p-1} \equiv 1 \pmod{p}, \text{ d. h. } a^{p-1} = 1 + hp$$

ist, wo h eine ganze Zahl bedeutet. Erheben wir diese Gleichung zur $p$ten Potenz und entwickeln die rechte Seite wieder nach dem binomischen Satze, so zeigt sich, dass alle Glieder mit Ausnahme des ersten Multipla von p^2 sind; wir erhalten daher

$$a^{(p-1)p} = 1 + h'p^2 \text{ oder } a^{(p-1)p} \equiv 1 \pmod{p^2},$$

wo wieder h' eine ganze Zahl bedeutet. So kann man fortfahren, indem man jedesmal wieder zur $p$ten Potenz erhebt, und gelangt auf diese Weise zu der Congruenz

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

deren Allgemeingültigkeit sich in derselben Weise durch den Schluss von π auf $\pi + 1$ nachweisen lässt.

Sind nun r, s . . . ebenfalls Primzahlen, welche nicht in a aufgehen, so ist nach demselben Satze

$$a^{(r-1)r^{\varrho-1}} \equiv 1 \pmod{r^\varrho}, \quad a^{(s-1)s^{\sigma-1}} \equiv 1 \pmod{s^\sigma} \ldots$$

Setzen wir ferner zur Abkürzung

$$h = (p-1)p^{\pi-1} \cdot (r-1)r^{\varrho-1} \cdot (s-1)s^{\sigma-1} \ldots$$

und berücksichtigen wir, dass aus jeder Congruenz von der Form

$$a^{\alpha} \equiv 1 \pmod{m}$$

auch die Congruenz

$$a^{h} \equiv 1 \pmod{m}$$

folgt, sobald h ein Multiplum von α ist, so ergiebt sich, dass die Congruenz

$$a^{h} \equiv 1$$

für jeden der Moduln p^{π}, r^{ϱ}, s^{σ} ... und folglich, da dieselben relative Primzahlen sind, auch für den Modul

$$k = p^{\pi} r^{\varrho} s^{\sigma} \ldots$$

gilt. Hiermit ist also von Neuem der verallgemeinerte Fermat'sche Satz erwiesen.

§. 21.

Es kommt häufig vor, dass eine oder beide Seiten einer Congruenz eine oder mehrere unbestimmte Zahlen $x, y \ldots$ enthalten, und es wird dann die Aufgabe gestellt, alle ganzzahligen Werthe von $x, y \ldots$ zu suchen, durch welche die beiden Seiten der Congruenz wirklich einander congruent werden. Je nach der Anzahl der Unbestimmten $x, y \ldots$ heisst dann eine solche Congruenz eine Congruenz mit einer, zwei oder mehreren *Unbekannten*, ähnlich wie dies bei Gleichungen zu geschehen pflegt. Auch hier nennt man dann solche specielle Werthe von $x, y \ldots$, welche die Congruenz zu einer identischen machen, *Wurzeln* der Congruenz, und das Problem der Auflösung einer Congruenz besteht in der Auffindung ihrer sämmtlichen Wurzeln. Wir werden im Folgenden nur solche Congruenzen betrachten, welche eine einzige Unbekannte x enthalten und ausserdem sich auf die Form

$$ax^{m} + bx^{m-1} + \cdots + gx + h \equiv 0 \pmod{k}$$

bringen lassen, worin m eine positive ganze Zahl und $a, b \ldots g, h$ ebenfalls gegebene ganze Zahlen bedeuten. Jeder Werth von x, der, in die linke Seite eingesetzt, dieselbe durch den Modul k theilbar macht, heisst also eine Wurzel dieser Congruenz. Kennt man irgend eine solche Wurzel x, so sind offenbar nach §. 17, 5. alle ihr nach dem Modul k congruenten Zahlen, d. h. alle Individuen der Classe, welcher diese Zahl x angehört, ebenfalls Wurzeln der-

selben Congruenz; man sieht alle solche einander congruenten Wurzeln daher nur wie eine einzige Wurzel an, und das Problem der vollständigen Auflösung der Congruenz kommt daher darauf zurück, alle unter einander *incongruenten* Wurzeln derselben aufzufinden.

Ferner leuchtet ein, dass jede Wurzel der obigen Congruenz, sobald

$$a \equiv a',\ b \equiv b' \ldots g \equiv g',\ h \equiv h' \pmod{k}$$

ist, auch eine Wurzel der Congruenz

$$a'x^m + b'x^{m-1} + \cdots + g'x + h' \equiv 0 \pmod{k}$$

sein wird, und umgekehrt. Beide Congruenzen sind daher auch nur wie eine und dieselbe anzusehen; denn beide stellen an die Unbekannte x genau dieselbe Forderung. Hieraus erhellt unmittelbar, dass man aus jeder Congruenz von der obigen Form ohne Weiteres alle diejenigen Glieder fortstreichen darf, deren Coefficienten durch den Modul theilbar sind; der Exponent der höchsten Potenz von x, welche nach dieser vorläufigen Ausscheidung zurückbleibt, heisst dann der *Grad* dieser Congruenz; ist z. B. in der obigen Congruenz der erste Coefficient a nicht durch den Modul k theilbar, so heisst dieselbe eine Congruenz $m$ten Grades.

Wenden wir diese Benennungen z. B. auf die Congruenz

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

an, so müssen wir sagen, dass dieselbe genau ebenso viele (incongruente) Wurzeln besitzt, als ihr Grad $\varphi(k)$ Einheiten enthält; denn erstens genügen alle relativen Primzahlen gegen den Modul der Congruenz, und diese zerfallen in $\varphi(k)$ Classen; und zweitens kann die Congruenz keine andern Wurzeln haben als diese; denn der grösste gemeinschaftliche Divisor δ einer Wurzel x und des Modul k ist auch gemeinschaftlicher Divisor der Zahlen $x^{\varphi(k)}$ und k, folglich auch (§. 18) der Zahlen 1 und k; folglich kann δ nur $= 1$ sein.

§. 22.

Wir wenden uns nun nach den vorhergehenden allgemeinen Erörterungen zu dem einfachsten speciellen Fall, nämlich zu der Congruenz ersten Grades, welcher man offenbar durch Transposition des bekannten Gliedes stets die Form

$$ax \equiv b \pmod{k} \qquad (1)$$

geben kann. Betrachten wir auch hier zunächst nur den speciellen Fall, in welchem der Coefficient a relative Primzahl gegen den Modul k ist, so ergiebt sich unmittelbar, dass diese Congruenz stets eine, aber auch nur eine Wurzel hat. Denn wir haben früher (§. 18) gesehen, dass die Werthe des Ausdrucks ax, welche man erhält, wenn man für x sämmtliche k Individuen eines vollständigen Systems incongruenter Zahlen einsetzt, wieder ein solches System bilden; unter den Werthen dieses Ausdrucks wird sich daher auch einer und nur einer finden, welcher derselben Classe angehört wie b, d. h. welcher $\equiv b$ ist. Der verallgemeinerte Fermat'sche Satz giebt nun auch ein Mittel an die Hand, die Wurzel dieser Congruenz unmittelbar zu bestimmen; offenbar genügt jede Zahl

$$x \equiv b \cdot a^{\varphi(k)-1} \pmod{k}$$

der obigen Congruenz. So findet man z. B., dass alle Wurzeln der Congruenz

$$2x \equiv -3 \pmod{15}$$

durch die Formel

$$x \equiv -3 \cdot 2^7 \equiv 6 \pmod{15}$$

gegeben werden.

Wenden wir uns nun dem allgemeinen Fall zu und nehmen wir an, es sei δ der grösste gemeinschaftliche Divisor des Coefficienten a und des Modul k, so leuchtet zunächst ein, dass, wenn die Congruenz überhaupt eine Wurzel x besitzt, auch b durch δ theilbar sein muss; denn da ax mit dem Modul k den gemeinschaftlichen Divisor δ hat, so muss auch $b \equiv ax$ durch δ theilbar sein. Dies ist also eine unerlässliche Bedingung für die Möglichkeit der Congruenz; dass sie auch hinreichend für dieselbe ist, wird sich sogleich zeigen.

Gesetzt nun, es sei x eine Wurzel der Congruenz, also

$$ax = b + mk,$$

wo m irgend eine ganze Zahl, so folgt hieraus, wenn $a = a'\delta$, $b = b'\delta$, $k = k'\delta$ gesetzt wird, $a'x = b' + mk'$, d. h. jede Wurzel der ursprünglichen Congruenz ist auch Wurzel der Congruenz

$$a'x \equiv b' \pmod{k'} \qquad (2)$$

und umgekehrt überzeugt man sich sogleich, dass jede Wurzel dieser letztern Congruenz auch eine Wurzel der erstern sein wird.

Die beiden Congruenzen (1) und (2) stimmen daher hinsichtlich ihrer Wurzeln vollständig mit einander überein; da nun in der letztern der Coefficient a' relative Primzahl gegen den Modul k' ist, so haben wir wieder den frühern Fall: diese Congruenz ist stets lösbar, und alle ihr genügenden Zahlen bilden in Bezug auf ihren Modul k' nur eine einzige Classe, in der Weise, dass, wenn α eine bestimmte derselben ist, alle andern in der Form

$$x = \alpha + zk' \qquad (3)$$

enthalten sind, wo z jede beliebige ganze Zahl bedeutet. Da nun alle diese Zahlen auch die sämmtlichen Wurzeln der Congruenz (1) bilden, so fragt es sich nur noch, wie viele in Bezug auf den Modul k incongruente Zahlen unter ihnen sich vorfinden. Irgend zwei in der Reihe (3) enthaltene Zahlen $\alpha + zk'$ und $\alpha + z'k'$ werden offenbar stets und auch nur dann congruent in Bezug auf den Modulus k sein, sobald $(z' - z)k'$ durch $k = k'\delta$, und also $z' - z$ durch δ theilbar ist; diese beiden Zahlen werden also einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modul k angehören, je nachdem die beiden Zahlen z und z' einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modulus δ angehören; woraus unmittelbar folgt, dass die Reihe (3) sämmtliche Individuen von δ verschiedenen Classen in Bezug auf den Modul k enthält, und es leuchtet ein, dass die folgenden δ Zahlen

$$\alpha,\ \alpha + k',\ \alpha + 2k' \ \ldots\ \alpha + (\delta - 1)k'$$

aus jeder dieser δ Classen einen Repräsentanten enthalten. Wir haben mithin folgendes allgemeine Resultat gewonnen:

Damit die Congruenz

$$ax \equiv b \pmod{k}$$

überhaupt Wurzeln besitze, ist erforderlich, dass b durch den grössten gemeinschaftlichen Divisor δ der beiden Zahlen a und k theilbar sei; ist diese Bedingung erfüllt, so hat die Congruenz genau δ incongruente Wurzeln.

Es ist zu bemerken, dass in dem früher behandelten Fall, in welchem $\delta = 1$ ist, die erforderliche Bedingung stets erfüllt ist, ferner, dass dieser Satz auch noch für den Fall $\delta = k$, in welchem also $a \equiv 0 \pmod{k}$ ist, seine Gültigkeit behält, indem, sobald b ebenfalls $\equiv 0 \pmod{k}$ ist, jede beliebige Zahl x dieser identischen Congruenz Genüge leistet.

Um auch ein Beispiel für den allgemeinen Fall zu behandeln, nehmen wir die Congruenz

$$8x \equiv -12 \pmod{60};$$

der grösste gemeinschaftliche Divisor des Coefficienten 8 und des Modul 60 ist hier $= 4$; da die rechte Seite -12 durch denselben theilbar ist, so ist sie möglich und wird 4 nach dem Modul 60 incongruente Wurzeln haben. Wir finden dieselben, indem wir zunächst die Wurzeln der entsprechenden Congruenz

$$2x \equiv -3 \pmod{15}$$

suchen; wir haben oben gesehen, dass dieselben in der Form

$$x \equiv 6 \pmod{15}$$

enthalten sind, und schliessen daraus, dass

$$x \equiv 6, \equiv 21, \equiv 36, \equiv 51 \pmod{60}$$

die vier Wurzeln der ursprünglichen Congruenz sind.

§. 23.

Obgleich im Vorhergehenden das Problem, zu entscheiden, ob eine vorgelegte Congruenz ersten Grades Wurzeln hat oder nicht, und im erstern Fall dieselben aufzufinden, eine vollständige Lösung gefunden hat, so ist dieselbe, sobald der Modul k eine grosse Zahl ist, wegen der erforderlichen Potenzirung für praktische Zwecke nicht wohl anwendbar; wir wollen daher im Folgenden eine einfachere Methode angeben. Offenbar können wir uns auf den Fall beschränken, in welchem der Coefficient der Unbekannten relative Primzahl gegen den Modul ist; ausserdem können wir annehmen, dass die rechte Seite $= 1$ ist; denn um aus der Wurzel einer solchen Congruenz diejenige einer andern zu finden, in welcher die rechte Seite eine andere Zahl ist, genügt es offenbar, dieselbe mit dieser Zahl zu multipliciren. Nennen wir der Bequemlichkeit halber den Modul nicht k, sondern b, so reducirt sich also unsere Aufgabe auf die Auflösung der Congruenz

$$ax \equiv 1 \pmod{b}$$

oder, was dasselbe ist, auf die Auflösung der unbestimmten Gleichung ersten Grades*)

$$ax - by = 1.$$

---

*) Die erste Lösung dieser Aufgabe findet sich bei *Bachet de Meziriac: Problèmes plaisans et délectables qui se font par les nombres.* 2e éd. 1624.

Wir schicken derselben einige Sätze über einen Algorithmus voraus, der zuerst von *Euler**) behandelt und für die Theorie der Kettenbrüche, sowie auch für unsere spätern Untersuchungen von Wichtigkeit ist. Es seien

$$a, b \tag{1}$$

irgend zwei unbestimmte Grössen, und ebenso

$$\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu \tag{2}$$

eine Reihe von beliebig vielen unbestimmten Grössen. Aus diesen bilden wir nun successive eine neue Reihe $c, d, e \ldots l, m, n$ nach folgendem Gesetz:

$$\left.\begin{aligned} c &= \gamma b + a \\ d &= \delta c + b \\ e &= \varepsilon d + c \\ &\cdots\cdots \\ n &= \nu m + l \end{aligned}\right\} \tag{3}$$

Substituirt man den Ausdruck für c in den für d, so wird der letztere eine ähnliche Form annehmen wie der erstere, nämlich

$$d = \delta a + (\gamma\delta + 1)b;$$

er besteht also aus einem Gliede, welches den Factor a, und aus einem zweiten, welches den Factor b enthält. Substituirt man nun diesen Ausdruck für d, und den ersten für c in den Ausdruck für e, so nimmt auch dieser letztere dieselbe Form an. So kann man fortfahren, und aus dem Ausdruck für n erkennt man, dass dieses Gesetz allgemein ist; denn sobald l und m schon diese Form erhalten haben, so nimmt auch n dieselbe an. Wir können daher

$$n = Ga + Hb$$

setzen, wo nun G und H unabhängig von a und b sein werden. Man bezeichnet den Coefficienten H, der nur von den in der Reihe (2) befindlichen Grössen abhängt, durch das Zeichen**)

$$[\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu], \tag{4}$$

und wir werden im Folgenden einige interessante Sätze beweisen, die sich auf dasselbe beziehen.

---

*) *Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus, relinquat data residua*, Comm. Ac. Petrop. VII, p. 46. — *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI, p. 28. — Vergl. *Gauss: D. A.* art. 27.

**) *Gauss: D. A.* art. 27.

Zunächst leuchtet ein, dass, wenn man mit den Anfangsgliedern

$$b,\ c = \gamma b + a \tag{1'}$$

und der Reihe

$$\delta,\ \varepsilon \ldots \lambda,\ \mu,\ \nu \tag{2'}$$

in derselben Weise verfährt wie oben, man genau dieselben Glieder $d, e \ldots l, m, n$ erhalten wird. Wir können daher gleichzeitig

$$n = Ga + [\gamma, \delta, \varepsilon \ldots \mu, \nu]b$$

und

$$n = G'b + [\delta, \varepsilon \ldots \mu, \nu]c$$

setzen; ersetzen wir hierin c durch $\gamma b + a$, so erhalten wir

$$n = [\delta, \varepsilon \ldots \mu, \nu]\ a + (\gamma[\delta, \varepsilon \ldots \mu, \nu] + G')b,$$

woraus, durch Vergleichung der Coefficienten von a in den beiden Formen für n, zunächst

$$G = [\delta, \varepsilon \ldots \mu, \nu]$$

folgt. Der Coefficient G lässt sich daher durch dasselbe Zeichen ausdrücken wie H. Wir können also von jetzt an schreiben

$$n = [\delta \ldots \mu, \nu]a + [\gamma, \delta \ldots \mu, \nu]b;$$

da nun auch

$$G' = [\varepsilon \ldots \mu, \nu]$$

sein muss, so erhalten wir durch Vergleichung der Coefficienten von b in den beiden Formen für n den Satz

$$[\gamma, \delta, \varepsilon \ldots \nu] = \gamma[\delta, \varepsilon \ldots \nu] + [\varepsilon \ldots \nu], \tag{5}$$

in welchem das Gesetz ausgedrückt ist, nach welchem die Fortbildung der Ausdrücke von der Form (4) nach links hin geschieht.

Einen ganz analogen Satz für die Fortbildung nach rechts hin erhält man durch die einfache Bemerkung, dass durch die Annahme $a = 0$, $b = 1$ die drei Grössen l, m, n resp. in

$$[\gamma \ldots \lambda],\ [\gamma \ldots \lambda, \mu],\ [\gamma \ldots \lambda, \mu, \nu]$$

übergehen, so dass zwischen diesen drei consecutiven Ausdrücken die Relation

$$[\gamma \ldots \lambda, \mu, \nu] = [\gamma \ldots \lambda, \mu]\nu + [\gamma \ldots \lambda] \tag{6}$$

besteht.

Verbindet man diese beiden Sätze mit einander, so überzeugt man sich leicht von der Richtigkeit des folgenden:

$$[\nu, \mu \ldots \delta, \gamma] = [\gamma, \delta \ldots \mu, \nu]. \tag{7}$$

Nimmt man nämlich an, dieser Satz sei für alle Ausdrücke dieser Art bewiesen, welche eine kleinere Anzahl von Grössen enthalten, so dass also z. B.

$$[\delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta] \text{ und } [\varepsilon \ldots \nu] = [\nu \ldots \varepsilon],$$

so folgt aus (5):

$$[\gamma, \delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta]\gamma + [\nu \ldots \varepsilon];$$

verbindet man dies mit dem Satz (6), so ergiebt sich unmittelbar die Richtigkeit der Gleichung (7). In der That gilt aber der Satz wirklich für die ersten Fälle; enthält nämlich der Ausdruck nur eine einzige Grösse γ, so versteht sich dies von selbst; und ausserdem ist

$$[\gamma, \delta] = \gamma\delta + 1 = [\delta, \gamma].$$

Hieraus folgt also, dass der Satz auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gilt.

Wir können die Gleichungen (3), durch welche das Bildungsgesetz der Grössen $c, d \ldots n$ ausgedrückt wird, auch in folgender Weise schreiben:

$$\begin{aligned} -c &= (-\gamma)b + (-a) \\ +d &= (-\delta)\,(-c) + b \\ -e &= (-\varepsilon)d + (-c) \\ &\cdots\cdots\cdots \\ \pm n &= (-\nu)\,(\mp m) + (\pm l) \end{aligned}$$

wo in der letzten Gleichung das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Hieraus geht hervor, dass aus den Anfangsgliedern

$$-a, b \qquad (1'')$$

und der Reihe

$$-\gamma, -\delta, -\varepsilon \ldots -\lambda, -\mu, -\nu \qquad (2'')$$

durch dasselbe frühere Verfahren die Reihe

$$-c, +d, -e \ldots \pm n$$

entsteht. Es wird daher auch

$$\pm n = [-\delta, -\varepsilon \ldots -\nu]\,(-a) + [-\gamma, -\delta, -\varepsilon \ldots -\nu]b$$

und folglich

$$[-\gamma, -\delta \ldots -\nu] = \pm[\gamma, \delta \ldots \nu] \qquad (8)$$

sein, worin wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \nu$ gerade oder ungerade ist.

Endlich kann man die Gleichungen (3) auch in umgekehrter Folge so schreiben:

$$l = (-\nu)m + n$$
$$k = (-\mu)l + m$$
$$\cdots\cdots\cdots$$
$$b = (-\delta)c + d$$
$$a = (-\gamma)b + c$$

Es wird daher

$$a = [-\mu \ldots -\gamma]n + [-\nu, -\mu \ldots -\gamma]m$$

oder mit Hülfe des Satzes (8):

$$\pm a = -[\mu \ldots \gamma]n + [\nu, \mu \ldots \gamma]m$$

oder mit Berücksichtigung des Satzes (7):

$$\pm a = -[\gamma, \delta \ldots \mu]n + [\gamma, \delta \ldots \mu, \nu]m.$$

Wenn man nun $a = 1$, $b = 0$ setzt, so gehen m, n resp. in

$$[\delta \ldots \mu], \quad [\delta \ldots \mu, \nu]$$

über, und man erhält das Resultat:

$$[\delta \ldots \mu]\,[\gamma, \delta \ldots \mu, \nu] - [\delta \ldots \mu, \nu]\,[\gamma, \delta \ldots \mu] = \pm 1, \qquad (9)$$

wo wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist.

Zum Schluss wollen wir bemerken, dass diese Ausdrücke in der Theorie der Kettenbrüche von der grössten Wichtigkeit sind; bezeichnen wir nämlich einen gewöhnlichen Kettenbruch, in welchem die Zähler sämmtlich $= 1$, und dessen sogenannte Quotienten $\gamma, \delta \ldots \mu, \nu$ sind, kurz durch das Symbol $(\gamma, \delta \ldots \mu, \nu)$, so dass also

$$(\gamma, \delta \ldots \lambda, \mu, \nu) = \gamma + \frac{1}{(\delta \ldots \lambda, \mu, \nu)} = \left(\gamma, \delta \ldots \lambda, \mu + \frac{1}{\nu}\right)$$

ist, so ergiebt sich allgemein durch Reduction desselben

$$(\gamma, \delta \ldots \mu, \nu) = \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]}. \qquad (10)$$

Denn gesetzt, dieser Satz sei schon für jede kleinere Anzahl der Grössen $\gamma, \delta, \varepsilon \ldots \mu', \nu$ bewiesen, so dass also namentlich

$$(\delta, \varepsilon \ldots \mu, \nu) = \frac{[\delta, \varepsilon \ldots \mu, \nu]}{[\varepsilon \ldots \mu, \nu]}$$

ist, so folgt hieraus

$$(\gamma, \delta, \varepsilon \ldots \mu, \nu) = \gamma + \frac{1}{(\delta, \varepsilon \ldots \mu, \nu)}$$
$$= \gamma + \frac{[\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]} = \frac{\gamma\,[\delta, \varepsilon \ldots \mu, \nu] + [\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]}$$

und hieraus ergiebt sich mit Berücksichtigung des Satzes (5) die Gleichung (10). In der That ist aber

$$(\gamma, \delta) = \gamma + \frac{1}{\delta} = \frac{\gamma\delta + 1}{\delta} = \frac{[\gamma, \delta]}{[\delta]};$$

da also der Satz für zwei Grössen γ, δ richtig ist, so ist er auch für jede beliebige Anzahl der Grössen γ, $\delta \ldots \mu$, ν richtig.

Sind die Elemente γ, $\delta \ldots \mu$, ν ganze Zahlen, so gilt dasselbe von den Zählern und Nennern der Brüche

$$\frac{[\gamma]}{1}, \frac{[\gamma, \delta]}{[\delta]} \ldots \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]};$$

ferner ist jeder dieser Brüche irreductibel, d. h. durch die kleinsten Zahlen ausgedrückt; denn es folgt z. B. aus der Relation (9), dass Zähler und Nenner des letzten der obigen Brüche ohne gemeinschaftlichen Divisor sind.

§. 24.

Die vorstehenden Sätze, welche eigentlich in die Theorie der Differenzen-Gleichungen zweiter Ordnung*) gehören, sind deshalb gleich in solcher Vollständigkeit aufgestellt, damit wir bei einer spätern Untersuchung nicht nöthig haben, von Neuem auf denselben Algorithmus zurückzukommen; für unsern nächsten Bedarf, nämlich für die Lösung der unbestimmten Gleichung

$$ax - by = 1,$$

in welcher wir nun wieder a und b als zwei gegebene relative Primzahlen ansehen, genügt schon ein kleiner Theil der vorhergehenden Resultate. Zu dem Zweck verfahren wir nun, wie es bei der Aufsuchung des grössten gemeinschaftlichen Divisors der beiden Zahlen (oder bei der Verwandlung des Bruches $a:b$ in einen Kettenbruch) geschieht, indem wir das System der folgenden Gleichungen bilden

$$\begin{aligned} a &= \gamma b + c \\ b &= \delta c + d \\ &\cdots\cdots \\ l &= \nu m + 1 \end{aligned}$$

wobei zuletzt der Rest 1 auftreten muss (§. 5); diese Gleichungen können wir auch so schreiben

*) Vergl. *Jacobi: Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus Drei vorhergehenden gebildet wird*, Crelle's Journal Bd. LXIX.

$$c = (-\gamma)b + a$$
$$d = (-\delta)c + b$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$1 = (-\nu)m + l$$

und hieraus folgt, dass

$$1 = [-\delta, -\varepsilon \cdots -\mu, -\nu]a + [-\gamma, -\delta, -\varepsilon \cdots -\mu, -\nu]b$$

oder nach §. 23, (8)

$$1 = \mp[\delta, \varepsilon \ldots \mu, \nu]a \pm [\gamma, \delta, \varepsilon \ldots \mu, \nu]b$$

ist, worin das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Wir erhalten daher folgende Auflösung der unbestimmten Gleichung:

$$x = \mp[\delta, \varepsilon \ldots \mu, \nu], \quad y = \mp[\gamma, \delta, \varepsilon \ldots \mu, \nu].$$

Hiermit ist also auch eine Wurzel x der Congruenz

$$ax \equiv 1 \pmod{b}$$

gefunden, und dies genügt vollständig, da alle anderen dieser einen nach dem Modul b congruent sind*).

Wenden wir diese Methode auf unser Beispiel

$$2x \equiv 1 \pmod{15}$$

an, so erhalten wir

$$2 = 0 \cdot 15 + 2, \quad 15 = 7 \cdot 2 + 1$$

also

$$\gamma = 0, \ \delta = 7, \quad x \equiv -[\delta] \equiv -7 \equiv 8 \pmod{15}$$

und hieraus folgt, dass

$$x \equiv -7 \cdot (-3) \equiv 21 \equiv 6 \pmod{15}$$

die Wurzel der Congruenz

$$2x \equiv -3 \pmod{15}$$

ist.

Als zweites Beispiel wählen wir die Congruenz

$$37x \equiv 1 \pmod{100};$$

indem wir ebenso verfahren, erhalten wir

$$37 = 0 \cdot 100 + 37; \quad 100 = 2 \cdot 37 + 26; \quad 37 = 1 \cdot 26 + 11;$$
$$26 = 2 \cdot 11 + 4; \quad 11 = 2 \cdot 4 + 3; \quad 4 = 1 \cdot 3 + 1$$

*) Man überzeugt sich leicht, dass aus einer Lösung x_0, y_0 alle anderen sich durch die Gleichungen $x = x_0 + bz$, $y = y_0 + az$ ableiten lassen, wo z eine willkürliche ganze Zahl bedeutet. Vergl. § 60.

und also

$$x \equiv - [2, 1, 2, 2, 1] \text{ (mod. } 100).$$

Nun ist, wenn wir von rechts nach links rechnen,

$$[1] = 1, [2, 1] = 3, [2, 2, 1] = 7, [1, 2, 2, 1] = 10,$$
$$[2, 1, 2, 2, 1] = 27,$$

also

$$x \equiv - 27 \equiv 73 \text{ (mod. } 100).$$

Da $\varphi(100) = \varphi(4)\,\varphi(25) = 2 \cdot 20 = 40$ ist, so hätten wir nach unserer früheren Methode die Auflösung

$$x \equiv 37^{39} \text{ (mod. } 100)$$

erhalten; die hierin angedeutete Rechnung würde sich zwar durch einige Kunstgriffe bedeutend abkürzen lassen, allein doch viel langwieriger sein als die nach der zweiten Methode ausgeführte Rechnung.

Kommt es darauf an, auch den Werth von

$$y = \mp [\gamma, \delta, \varepsilon \ldots \mu, \nu]$$

zu berechnen, so ist es vortheilhaft, die Berechnung des Werthes

$$x = \mp [\delta, \varepsilon \ldots \mu, \nu]$$

von rechts nach links vorzunehmen; man findet dann nach der Formel (5) des §. 23 aus

$$[\varepsilon \ldots \mu, \nu] \text{ und } [\delta, \varepsilon \ldots \mu, \nu]$$

unmittelbar den Werth von y. So oft $\gamma = 0$, also $a < b$ ist, reducirt sich y auf

$$y = \mp [\varepsilon \ldots \mu, \nu].$$

Dies ist in unseren Beispielen der Fall; in dem zweiten erhält man auf diese Weise

$$y = - [0, 2, 1, 2, 2, 1] = - [1, 2, 2, 1] = - 10,$$

und in der That ist

$$37 \cdot (-27) - 100 \cdot (-10) = 1.$$

Bei dieser Lösung der unbestimmten Gleichung $ax - by = 1$ in ganzen Zahlen x, y war stillschweigend vorausgesetzt, dass die beiden gegebenen relativen Primzahlen a, b *positive* Zahlen sind; doch erkennt man leicht, dass hierdurch die Allgemeinheit der Lösung nicht beeinträchtigt wird.

Wir bemerken ferner, dass durch wiederholte Anwendung desselben Verfahrens folgende allgemeinere Aufgabe gelöst werden kann: *Sind a, b, c ... gegebene ganze Zahlen, deren grösster ge-*

meinschaftlicher Divisor m ist, so sollen ebensoviele ganze Zahlen $x, y, z \ldots$ gefunden werden, welche der Gleichung

$$ax + by + cz + \cdots = m$$

genügen. Denn gesetzt, man habe für die Zahlen $b, c \ldots$, deren grösster gemeinschaftlicher Divisor m' nothwendig ein Multiplum von m ist, schon ganze Zahlen $y', z' \ldots$ gefunden, welche der Bedingung

$$by' + cz' + \cdots = m'$$

genügen, so löse man, da m der grösste gemeinschaftliche Divisor von a und m' ist, nach der obigen Methode die Gleichung

$$ax + m'x' = m$$

in ganzen Zahlen x, x', so wird die vorgelegte Gleichung durch die Zahlen $x, y = x'y', z = x'z' \ldots$ befriedigt.

§. 25.

Auf das im Vorhergehenden behandelte Problem der Auflösung der Congruenzen ersten Grades lässt sich das folgende zurückführen:

Alle Zahlen x zu finden, welche in Bezug auf zwei gegebene Moduln a, b gegebenen Zahlen resp. α, β congruent sind, d. h. welche den beiden Forderungen

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}$$

genügen.

Da nämlich alle Zahlen x, welche die erste dieser beiden Forderungen erfüllen, in der Form $x = \alpha + at$ enthalten sind, wo t jede beliebige ganze Zahl bedeutet, so kommt es nur noch darauf an, dieses t näher so zu bestimmen, dass

$$at \equiv \beta - \alpha \pmod{b} \qquad (1)$$

wird. Bezeichnet man nun mit δ den grössten gemeinschaftlichen Divisor der beiden Moduln a und b, so muss, wenn diese Congruenz möglich sein soll, $\beta - \alpha$ durch δ theilbar, d. h. es muss

$$\alpha \equiv \beta \pmod{\delta} \qquad (2)$$

sein. Ist diese Bedingung nicht erfüllt, so existirt keine Zahl, welche der Aufgabe genügt; ist sie aber erfüllt, so sind sämmtliche der Congruenz (1) genügende Zahlen t in der Form

$$t \equiv \gamma \left(\text{mod. } \frac{b}{\delta}\right) \text{ oder } t = \gamma + \frac{b}{\delta} u$$

enthalten, wo γ eine bestimmte von ihnen, und u jede beliebige ganze Zahl bedeutet. Hieraus folgt, dass die gesuchten Zahlen durch die Formel

$$x = \alpha + \gamma a + \frac{ab}{\delta} u \text{ oder } x \equiv x_0 \left(\text{mod. } \frac{ab}{\delta}\right)$$

gegeben werden, wo $x_0 = \alpha + \gamma a$ selbst eine der gesuchten Zahlen, und der Modulus offenbar das kleinste gemeinschaftliche Multiplum der beiden gegebenen Moduln a, b ist.

Werden z. B. die Zahlen gesucht, welche durch 12 dividirt den Rest 7, durch 15 dividirt den Rest 4 lassen, so hat man die Congruenzen

$$x \equiv 7 \text{ (mod. 12)}, \quad x \equiv 4 \text{ (mod. 15)}.$$

Man setzt also $x = 7 + 12t$, und erhält für t die Congruenz

$$12t \equiv -3 \text{ (mod. 15)},$$

welche (da hier die Bedingung (2) erfüllt ist) sich auf

$$4t \equiv -1 \text{ (mod. 5)}$$

reducirt. Hieraus folgt

$$t \equiv 1 \text{ (mod. 5)}$$

und also

$$x = 7 + 12t \equiv 19 \text{ (mod. 60)}.$$

Besonders bemerkenswerth ist der besondere Fall, in welchem die beiden gegebenen Moduln a, b relative Primzahlen sind; da gleichzeitig $\delta = 1$ wird, so fällt die Bedingung (2) ganz fort; die Auflösung ist stets möglich und liefert ein Resultat von der Form

$$x \equiv \mu x_0 \text{ (mod. } ab).$$

Die ursprüngliche Aufgabe lässt sich auch leicht für den Fall verallgemeinern, in welchem eine Reihe von beliebig vielen Moduln und eine Reihe ihnen entsprechender Reste gegeben ist; für uns ist indessen nur der Fall von Wichtigkeit, in welchem die gegebenen Moduln a, b, c . . . relative Primzahlen sind; wir beschränken uns daher auf denselben, und stellen uns unter dieser Voraussetzung die Aufgabe, alle Zahlen x zu finden, welche dem System von Congruenzen

$$x \equiv \alpha \text{ (mod. } a), \quad x \equiv \beta \text{ (mod. } b), \quad x \equiv \gamma \text{ (mod. } c) \ldots$$

genügen. Da wir nun schon wissen, dass alle Zahlen, welche die beiden ersten dieser Forderungen erfüllen, in der Form $x \equiv \beta_1$ (mod. ab)

enthalten sind, wo die Zahl β_1 nach dem Vorhergehenden gefunden werden kann, so kommt unsere Aufgabe offenbar auf die einfachere zurück, alle Zahlen x zu finden, welche dem folgenden System von Congruenzen genügen:

$$x \equiv \beta_1 \pmod{ab}, \quad x \equiv \gamma \pmod{c} \ldots$$

Da nun der Modul ab der ersten dieser Congruenzen wieder relative Primzahl gegen jeden folgenden Modul $c \ldots$ ist, so kann man in derselben Weise fortfahren und gelangt so zu dem Resultat, dass sämmtliche Zahlen x in der Form

$$x \equiv x_0 \pmod{m}$$

enthalten sind, wo x_0 eine bestimmte von ihnen, und m das Product $abc \ldots$ aus allen gegebenen Moduln bedeutet.

Statt eine solche Zahl x_0 in der eben angegebenen Weise durch successive Auflösung einer Reihe von Congruenzen ersten Grades in Bezug auf die Moduln $b, c \ldots$ zu suchen, kann man auch auf folgende Art symmetrisch verfahren.

Man setze $m = aA = bB = cC \ldots$ und bestimme (nach §. 24) zunächst Zahlen $a', b', c' \ldots$, welche den Congruenzen

$$Aa' \equiv 1 \pmod{a}, \quad Bb' \equiv 1 \pmod{b}, \quad Cc' \equiv 1 \pmod{c} \ldots$$

genügen; so wird

$$x \equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots \pmod{m};$$

denn da $B, C \ldots$ durch a theilbar sind, so ist $x \equiv Aa'\alpha \equiv \alpha \pmod{a}$, und ebenso $\equiv \beta \pmod{b}$, $\equiv \gamma \pmod{c}$ u. s. w.

Ein besonderer Vortheil dieser Methode besteht darin, dass die Hülfszahlen $a', b', c' \ldots$ ganz unabhängig von $\alpha, \beta, \gamma \ldots$ sind, und daher stets dieselben bleiben, wie auch die letzteren variiren mögen, vorausgesetzt natürlich, dass das System der Moduln $a, b, c \ldots$ unverändert bleibt.

Es folgt ferner hieraus, dass x ein vollständiges Restsystem nach dem Modul m durchläuft, sobald die Reste $\alpha, \beta, \gamma \ldots$ vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c \ldots$ durchlaufen; denn wenn $\alpha', \beta', \gamma' \ldots$ irgend ein zweites System gegebener Reste ist, so wird

$$Aa'\alpha' + Bb'\beta' + Cc'\gamma' + \cdots$$

stets und nur dann

$$\equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots$$

nach dem Modulus m sein, wenn gleichzeitig

$$\alpha' \equiv \alpha \pmod{a}, \quad \beta' \equiv \beta \pmod{b}, \quad \gamma' \equiv \gamma \pmod{c}$$

u. s. w. ist; da ferner $\alpha, \beta, \gamma \ldots$ resp. $a, b, c \ldots$ verschiedene Werthe durchlaufen, so ist die Anzahl aller verschiedenen Restsysteme, also auch die Anzahl der resultirenden nach dem Modul m incongruenten Werthe von x gleich $abc \ldots = m$; d. h. x durchläuft ein vollständiges Restsystem nach dem Modul m.

Ist ferner α relative Primzahl zu a, β zu b u. s. f., so ist x auch relative Primzahl zu m, und umgekehrt; hieraus folgt leicht ein neuer Beweis des Satzes, dass $\varphi(ab) = \varphi(a)\,\varphi(b)$ ist.

Endlich ergiebt sich, dass, wenn x irgend eine ganze Zahl bedeutet, stets

$$\frac{x}{m} = h + \frac{u}{a} + \frac{v}{b} + \frac{w}{c} + \cdots$$

gesetzt werden kann, wo $h, u, v, w \ldots$ ganze Zahlen bedeuten. Denn lässt x in Bezug auf die Moduln $a, b, c \ldots$ resp. die Reste $\alpha, \beta, \gamma \ldots$, so ist nach dem Obigen

$$x = hm + Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots,$$

wo h eine ganze Zahl bedeutet, und folglich

$$\frac{x}{m} = h + \frac{a'\alpha}{a} + \frac{b'\beta}{b} + \frac{c'\gamma}{c} + \cdots$$

§. 26.

Wir wenden uns nun zu der Betrachtung der Congruenzen höherer Grade, beschränken uns aber dabei auf den einfachsten Fall, in welchem der Modul p eine *Primzahl* ist. Die allgemeinste Form einer Congruenz $n$ten Grades ist die folgende:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + h \equiv 0 \pmod{p},$$

in welcher der höchste Coefficient a als nicht theilbar durch die Primzahl p vorausgesetzt wird. Ebenso wie man jede Gleichung leicht auf den Fall zurückführen kann, in welchem der höchste Coefficient $= 1$ ist, so erreicht man auch hier dasselbe, wenn man die Congruenz mit einer Zahl a' multiplicirt, welche der Bedingung $aa' \equiv 1 \pmod{p}$ genügt und also eine Wurzel der stets lösbaren Congruenz $ax \equiv 1 \pmod{p}$ ist. Doch hängt hiervon die Gültigkeit der folgenden Sätze nicht im Mindesten ab.

Wir bezeichnen der Einfachheit halber das auf der linken Seite der obigen Congruenz befindliche Polynom $n$ten Grades kurz mit $f(x)$. Hat nun eine solche Congruenz

$$f(x) \equiv 0 \pmod{p} \qquad (1)$$

eine Wurzel $x \equiv \alpha$ und dividirt man $f(x)$ durch $x - \alpha$, so wird der Divisionsrest r_1 eine durch p theilbare Zahl sein; denn bezeichnet man den Quotienten der Division, welcher eine ganze Function vom $(n-1)$ten Grade mit ganzzahligen Coefficienten ist, mit $f_1(x)$, so ist

$$f(x) = (x - \alpha) f_1(x) + r_1 \qquad (2)$$

und hierin ist $r_1 = f(\alpha)$ der Voraussetzung nach $\equiv 0 \pmod{p}$.

Hat nun die Congruenz (1) noch eine zweite von α verschiedene, d. h. nicht mit α congruente Wurzel β, so folgt aus (2), dass

$$(\beta - \alpha) f_1(\beta) \equiv 0 \pmod{p}$$

und also, da $\beta - \alpha$ nicht durch p theilbar ist, dass $f_1(\beta) \equiv 0$, d. h. dass β eine Wurzel der Congruenz $f_1(x) \equiv 0 \pmod{p}$ sein muss. Man kann daher wieder

$$f_1(x) = (x - \beta) f_2(x) + r_2$$

setzen, wo der Rest r_2 wieder eine durch p theilbare Zahl, und der Quotient $f_2(x)$ eine ganze Function $(n-2)$ten Grades mit ganzzahligen Coefficienten ist. Setzt man aber diesen Ausdruck für $f_1(x)$ in die Gleichung (2) ein, so nimmt dieselbe die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + r_2 (x - \alpha) + r_1$$

oder, da r_1 und r_2 durch p theilbar sind, die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + p(lx + m)$$

an, in welcher l und m ganze Zahlen sind.

Besitzt nun die Congruenz (1) noch eine dritte von α und β verschiedene Wurzel γ, so ergiebt sich, da weder $(\gamma - \alpha)$ noch $(\gamma - \beta)$ durch p theilbar ist, dass γ eine Wurzel der Congruenz $f_2(x) \equiv 0$ ist; verfährt man daher wie früher, so erhält man eine Gleichung von der Form

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma) f_3(x) + p(rx^2 + sx + t),$$

wo r, s, t ganze Zahlen bedeuten. Setzt man diese Schlussweise fort, so gelangt man offenbar zu folgendem Satze: ***Besitzt die Congruenz $n$ten Grades***

$$f(x) \equiv 0 \pmod{p},$$

deren Modulus p eine Primzahl ist, n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so ist ihre linke Seite von der Form

$$f(x) = a(x - \alpha)(x - \beta)(x - \gamma) \ldots (x - \lambda) + p\psi(x), \qquad (3)$$

wo a den höchsten Coefficienten von $f(x)$, und $\psi(x)$ ein Polynom bedeutet, dessen Coefficienten ganze Zahlen sind.

Und aus diesem ersten Satze folgt sogleich der zweite*): *Eine Congruenz vom Grade n, deren Modulus eine Primzahl ist, kann niemals mehr als n incongruente Wurzeln haben.* Denn hätte die Congruenz (1) ausser den n Wurzeln $\alpha, \beta \ldots \lambda$ noch mindestens eine solche μ, die mit keiner der vorhergehenden congruent ist, so würde aus der Gleichung (3) folgen, dass das Product

$$a(\mu-\alpha)(\mu-\beta)(\mu-\gamma)\ldots(\mu-\lambda)$$

durch p theilbar wäre, was unmöglich ist, da der Voraussetzung nach keiner der Factoren durch p theilbar ist.

Man hätte diese beiden Sätze, welche für die Folge von der grössten Wichtigkeit sind, auch in umgekehrter Folge aus dem in der Gleichung (2) ausgesprochenen Resultat schliessen können. Da nämlich jede von α verschiedene Wurzel β der Congruenz (1) eine Wurzel der Congruenz nächst niedrigern Grades

$$f_1(x) \equiv 0 \pmod{p}$$

ist, so folgt hieraus unmittelbar, dass die erstere Congruenz höchstens eine Wurzel mehr besitzt, als die letztere; da nun eine Congruenz ersten Grades (sobald der Modulus eine Primzahl ist) nur eine Wurzel besitzt, so kann eine Congruenz vom zweiten Grade höchstens 2, folglich eine Congruenz dritten Grades höchstens 3 u. s. f., allgemein eine Congruenz $n$ten Grades höchstens n incongruente Wurzeln besitzen. Und nachdem so der zweite Satz bewiesen ist, ergiebt sich auch der erste leicht auf folgende Weise. Gesetzt, die Congruenz (1) vom $n$ten Grade hat wirklich n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so bilde man die Differenz

$$f(x) - a(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\lambda) = \varphi(x)$$

wo a den höchsten Coefficienten in $f(x)$ bezeichnet, und denke sich dieselbe nach Potenzen von x geordnet; dann ist zu zeigen, dass alle Coefficienten dieses Polynoms $\varphi(x)$, dessen Grad höchstens $= n-1$, also jedenfalls kleiner als n ist, durch p theilbar sind. Gesetzt, dies wäre nicht der Fall, und es wäre x^r die höchste in $\varphi(x)$ vorkommende Potenz von x, deren Coefficient nicht durch p theilbar wäre, so wäre

$$\varphi(x) \equiv 0 \pmod{p}$$

---

*) ***Lagrange:*** *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers,* Mém. de l'Ac. de Berlin. T. XXIV.

eine Congruenz vom $r$ten Grade, welche, wie man unmittelbar einsieht, die n incongruenten Zahlen $\alpha, \beta \ldots \lambda$ zu Wurzeln hätte, also, da $r < n$ ist, mehr Wurzeln besässe, als ihr Grad Einheiten enthält. Da dies gegen den schon bewiesenen Satz streitet, so müssen wirklich alle Coefficienten von $\varphi(x)$ durch p theilbar sein, d. h. es muss

$$\varphi(x) = p\,\psi(x)$$

sein, wo sämmtliche Coefficienten des Polynoms $\psi(x)$ ganze Zahlen sind. Dies war aber der Inhalt des ersten Satzes.

Wir können zu diesen beiden Sätzen noch den folgenden dritten hinzufügen: *Wenn*

$$f(x) = \varphi(x)\ \psi(x)$$

ist, wo die Coefficienten der Polynome $\varphi(x)$ und $\psi(x)$ sämmtlich ganze Zahlen sind, und wenn die Congruenz

$$f(x) \equiv 0 \pmod{p}, \tag{4}$$

(wo p wieder eine Primzahl bedeutet) ebenso viele incongruente Wurzeln besitzt, als ihr Grad Einheiten enthält, so gilt dasselbe von jeder der beiden Congruenzen

$$\varphi(x) \equiv 0 \pmod{p}, \quad \psi(x) \equiv 0 \pmod{p}. \tag{5}$$

Zunächst leuchtet nämlich ein, dass jede Wurzel α der Congruenz (4) auch eine Wurzel von mindestens einer der beiden Congruenzen (5) sein muss; denn aus

$$\varphi(\alpha)\ \psi(\alpha) = f(\alpha) \equiv 0 \pmod{p}$$

folgt, dass mindestens eine der beiden Zahlen $\varphi(\alpha)$, $\psi(\alpha)$ durch p tbeilbar sein muss. Hätte nun eine der beiden Congruenzen (5) weniger incongruente Wurzeln als ihr Grad Einheiten enthält, so müsste nothwendig die Anzahl der Wurzeln der andern Congruenz d. h. der übrigen Wurzeln der Congruenz (4) ihren Grad übersteigen, da die Summe der Grade der beiden Polynome $\varphi(x)$ und $\psi(x)$ genau dem Grade des Polynoms $f(x)$ gleich ist. Da dies gegen den zweiten Satz verstossen würde, so muss die Anzahl der incongruenten Wurzeln einer jeden der beiden Congruenzen (5) genau ihrem Grade gleich sein *).

*) Eine weitere Entwicklung dieses Gegenstandes findet man in des Herausgebers Abhandlung: *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, Crelle's Journal Bd. LIV. — Vergl. die nachgelassene Abhandlung von *Gauss: Analysis Residuorum*, Gauss' Werke Bd. II. 1863.

§. 27.

Von diesen wichtigen Sätzen machen wir sogleich eine Anwendung. Zufolge des Fermat'schen Satzes genügt jede der $(p-1)$ unter einander nach dem Modul p incongruenten Zahlen

$$1, 2, 3 \ldots (p-1)$$

der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

und diese Zahlen bilden auch ihre sämmtlichen incongruenten Wurzeln. Es ist daher nach dem ersten der vorhergehenden drei Sätze

$$x^{p-1} - 1 = (x-1)(x-2)(x-3) \ldots (x-p+1) + p\psi(x),$$

worin $\psi(x)$ ein Polynom mit ganzen Coefficienten bezeichnet. Entwickelt man daher das rechter Hand befindliche Product nach Potenzen von x, so muss der Coefficient einer jeden Potenz von x dem entsprechenden linker Hand in Bezug auf den Modul p congruent sein. Wir wollen hier nur den interessantesten Fall betrachten der sich durch die Vergleichung der Glieder ergiebt, welche von x unabhängig sind. Ist zunächst p eine *ungerade* Primzahl, so ist dieses Glied rechter Hand, da die Anzahl $p-1$ der negativen Factoren gerade ist,

$$= 1 \cdot 2 \cdot 3 \ldots (p-1),$$

linker Hand dagegen $= -1$, und hieraus ergiebt sich der nach *Wilson* benannte Satz:

Wenn p eine Primzahl bedeutet, so ist das um eine Einheit vergrösserte Product aller kleineren Zahlen als p durch p theilbar in Zeichen

$$1 \cdot 2 \ldots (p-1) \equiv -1 \pmod{p}.$$

So ist z. B.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721$$

theilbar durch 7.

Der Wilson'sche Satz gilt aber auch für die Primzahl 2, da in diesem Fall $+1$ und -1 einander congruent sind.

Dieser Satz ist dadurch bemerkenswerth, dass er sich umkehren lässt und deshalb ein charakteristisches Merkmal für eine Primzahl abgiebt. Denn nimmt man umgekehrt an, es sei

$$1 \cdot 2 \cdot 3 \ldots (p-1)+1$$

durch p theilbar, so muss p eine Primzahl sein; wäre nämlich p eine zusammengesetzte Zahl, also ausser durch 1 und durch sich selbst auch noch durch eine andere Zahl a theilbar, so würde a nothwendig eine der Zahlen 2, 3 . . $(p-1)$ sein müssen; da nun die obige Summe und ihr erstes Glied durch a theilbar ist, so müsste auch das zweite Glied 1 durch a theilbar sein, was nicht möglich ist.

Einen andern interessanten Satz erhält man durch Anwendung des dritten der vorhergehenden Sätze auf dasselbe Beispiel. Bezeichnet nämlich δ irgend einen Divisor von $p-1$, so ist bekanntlich

$$x^{p-1}-1 \doteq (x^{\delta}-1)\ \psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet. Hieraus folgt also: *Die Congruenz*

$$x^{\delta} \equiv 1 \pmod{p},$$

deren Grad δ ein Divisor von $p-1$ ist, besitzt stets δ incongruente Wurzeln.

§. 28.

Der zuletzt abgeleitete Satz gehört seinem Inhalte nach eigentlich in eine allgemeinere Theorie, nämlich in die Theorie der *binomischen Congruenzen* von der Form

$$a x^n \equiv b \pmod{k}.$$

Dieselbe stützt sich auf die Betrachtung der sogenannten *Potenzreste*, d. h. der Reste der successiven Potenzen einer Zahl, und wir beschäftigen uns daher zunächst mit der Untersuchung der interessanten Gesetze, welche hier hervortreten.

Es sei also k ein beliebiger Modul, und a relative Primzahl gegen denselben; bilden wir nun die Reihe

$$1, a, a^2, a^3 \ldots$$

der successiven Potenzen von a und setzen dieselbe hinreichend weit fort, so muss es einmal geschehen, dass zwei verschiedene Glieder a^s und a^{s+n} einander nach dem Modul k congruent werden; denn es giebt ja nur eine endliche Anzahl incongruenter Zahlen. Aus der Congruenz

$$a^{s+n} = a^s \,.\, a^n \equiv a^s \pmod{k}$$

folgt aber, da a^s relative Primzahl gegen den Modul k ist, dass

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

ist. Es giebt daher, was wir auch schon durch den verallgemeinerten Fermat'schen Satz (§. 19) wussten, stets eine Potenz von a, welche durch k dividirt den Rest 1 lässt. Unter allen Potenzen von a, welche dieselbe Eigenschaft haben, ist aber besonders diejenige bemerkenswerth, welche den kleinsten Exponenten hat; doch versteht sich von selbst, dass der Exponent Null hier nicht in Betracht kommt, für welchen die entsprechende Potenz ja stets $\equiv 1$ sein würde. Bezeichnen wir mit δ diesen kleinsten positiven Exponenten, für welchen

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

wird, so wollen wir sagen, die Zahl a *gehöre* zu dem Exponenten δ oder zu der Zahl δ. Dann leuchtet zunächst ein, dass die ersten δ Glieder der obigen Potenzreihe, d. h. die Zahlen

$$1, \quad a, \quad a^2 \ldots a^{\delta-1}$$

sämmtlich incongruent unter einander sind; denn aus einer Congruenz von der Form $a^{s+n} \equiv a^s$, wo s und $s+n$ kleiner als δ sind, würde wieder $a^n \equiv 1$ folgen, was mit der Voraussetzung im Widerspruch steht, dass keine niedrigere Potenz als a^δ den Rest 1 lässt.

Die folgenden Glieder der Reihe geben nun genau dieselben Reste, und auch in derselben Reihenfolge, denn es ist

$$\begin{aligned}
&a^\delta \equiv 1, \quad a^{\delta+1} \equiv a, \quad a^{\delta+2} \equiv a^2 \ldots a^{2\delta-1} \equiv a^{\delta-1} \\
&a^{2\delta} \equiv 1, \quad a^{2\delta+1} \equiv a, \quad a^{2\delta+2} \equiv a^2 \ldots a^{3\delta-1} \equiv a^{\delta-1} \\
&a^{3\delta} \equiv 1, \quad a^{3\delta+1} \equiv a, \quad a^{3\delta+2} \equiv a^2 \ldots a^{4\delta-1} \equiv a^{\delta-1}
\end{aligned}$$

u. s. w.

Um daher zu erfahren, welchen Rest eine beliebige Potenz a^s lässt, dividire man den Exponenten s durch δ und bringe dadurch s in die Form $s = m\delta + r$, wo r eine der Zahlen $0, 1, 2 \ldots (\delta - 1)$ bezeichnet. Dann ist

$$a^s = a^{m\delta+r} \equiv a^r \pmod{k}.$$

Hieraus geht ferner hervor, dass zwei solche Potenzen wie a^s und $a^{s'}$ stets, aber auch nur dann congruent sein werden in Bezug auf den Modul k, wenn $s \equiv s' \pmod{\delta}$; denn ist r' der bei der Division von s' durch δ hervorgehende Rest, so ist $a^{s'} \equiv a^{r'} \pmod{k}$. Ist daher

$$a^s \equiv a^{s'} \pmod{k}$$

so muss auch

$$a^r \equiv a^{r'} \pmod{k}$$

sein; da aber r und r' kleiner als δ sind, so ist dies nur dann möglich, wenn $r = r'$ ist, woraus $s \equiv s' \pmod{\delta}$ folgt; und umgekehrt leuchtet ein, dass, sobald $s \equiv s' \pmod{\delta}$, also $r = r'$ ist, auch $a^s \equiv a^{s'} \pmod{k}$ sein muss.

Ein specieller Fall ist der, dass, sobald $a^s \equiv 1$, also $a^s \equiv a^0$ ist, nothwendig $s \equiv 0 \pmod{\delta}$, d. h. dass s theilbar durch δ sein muss. Nun wissen wir schon aus dem verallgemeinerten Fermat'schen Satz, dass stets

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

ist; hieraus folgt also, dass die Zahl δ, zu welcher eine Zahl a gehört, stets ein Divisor von $\varphi(k)$ sein muss*).

§. 29.

Beschränken wir uns jetzt wieder auf den Fall, in welchem der Modul eine Primzahl p und also a irgend eine durch p nicht theilbare Zahl ist, so folgt aus der letzten Bemerkung, dass die Zahl δ, zu welcher a gehört, jedenfalls ein Divisor von $\varphi(p) = p - 1$ sein muss. Man kann nun umgekehrt fragen: wenn δ irgend ein Divisor von $p - 1$ ist, giebt es dann jedesmal auch Zahlen a, welche zu δ gehören? und wie viele? Nehmen wir zunächst einmal ein Beispiel, indem wir $p = 7$ setzen. Da aus $a \equiv a' \pmod{p}$ auch stets $a^s \equiv a'^s \pmod{p}$ folgt, so gehören je zwei congruente Zahlen auch stets zu demselben Exponenten, und wir brauchen daher in unserm Beispiel nur die Zahlen $a = 1, 2, 3, 4, 5, 6$ zu betrachten; durch wirkliches Potenziren, welches man dadurch abkürzt, dass man statt jeder Potenz immer ihren kleinsten Rest substituirt, findet man nun das in der folgenden Tabelle ausgedrückte Resultat:

a	1	2	3	4	5	6
δ	1	3	6	3	6	2

Es gehört daher zu dem Divisor $\delta = 1$ nur die einzige Zahl 1, zu $\delta = 2$ nur die einzige Zahl 6; zu $\delta = 3$ gehören zwei Zah-

*) Ein anderer Beweis dieses Satzes findet sich in den Supplementen V. §. 127.

len, nämlich 2 und 4, und zu $\delta = 6$ gehören die beiden Zahlen 3 und 5.

Nehmen wir nun vorläufig einmal an, dass *mindestens eine* Zahl a existirt, welche zu dem Exponenten δ gehört, so sind die δ Zahlen

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

nach dem Vorhergehenden sämmtlich incongruent; da ferner $a^\delta \equiv 1$, so ist auch

$$(a^r)^\delta = (a^\delta)^r \equiv 1 \pmod{p},$$

d. h. die δ Zahlen (A) sind Wurzeln der Congruenz

$$x^\delta \equiv 1 \pmod{p},$$

und da sie unter einander incongruent sind, und der Modulus eine Primzahl ist, so bilden sie auch die sämmtlichen Wurzeln dieser Congruenz vom Grade δ. Jede Zahl aber, welche zum Exponenten δ gehört, muss vor Allem eine Wurzel dieser Congruenz sein, und wir haben daher alle etwa existirenden Zahlen, die zu δ gehören, unter den Zahlen (A) zu suchen. Wir fragen daher: zu welchem Exponenten h gehört irgend eine dieser Zahlen, z. B. a^r? d. h. welches ist die kleinste positive Zahl h, für welche

$$(a^r)^h = a^{rh} \equiv 1 \pmod{p}$$

ist? Offenbar muss rh (da a zum Exponenten δ gehört) durch δ theilbar sein; ist daher ε der grösste gemeinschaftliche Divisor von r und $\delta = \varepsilon\delta'$, so muss h durch δ' theilbar sein; die kleinste Zahl h, welche diese Bedingung erfüllt, ist offenbar δ' selbst, und dann ist auch wirklich

$$(a^r)^h = (a^\delta)^{\frac{r}{\varepsilon}} \equiv 1 \pmod{p};$$

also ist δ' die Zahl, zu welcher a^r gehört. Soll also a^r zum Exponenten δ gehören, so muss $\varepsilon = 1$, also r relative Primzahl gegen δ sein; und umgekehrt, sobald dies der Fall, also $\varepsilon = 1$ ist, gehört auch a^r wirklich zum Exponenten δ. Wir erhalten so das Resultat, dass unter den Zahlen (A) genau ebenso viele zu dem Exponenten δ gehören, als es unter den Exponenten

$$0,\ 1,\ 2 \ldots (\delta - 1)$$

relative Primzahlen zu δ giebt; es giebt daher $\varphi(\delta)$ solche Zahlen.

Da wir angenommen hatten, dass *mindestens eine* solche Zahl a existirte, so können wir das Bisherige so zusammenfassen: Ist p eine Primzahl und δ ein Divisor von $p-1$, so ist die Anzahl

der incongruenten Zahlen, die zu δ gehören, entweder $= 0$, oder $= \varphi(\delta)$. Um nun über diese Alternative zu entscheiden, betrachten wir die Totalität aller $p-1$ nach dem Modul p incongruenten und durch p nicht theilbaren Zahlen; wir theilen dieselben in Gruppen ein, indem wir je zwei incongruente Zahlen in dieselbe oder in verschiedene Gruppen werfen, je nachdem sie zu demselben Divisor δ von $p-1$ gehören oder zu verschiedenen. Bezeichnen wir mit $\psi(\delta)$ die Anzahl der Individuen, welche in die dem Divisor δ entsprechende Gruppe gehören, so muss, da jede der $p-1$ vertheilten Zahlen in eine, aber auch nur in eine solche Gruppe gehört,

$$\Sigma \psi(\delta) = p-1$$

sein, wo sich das Summenzeichen auf sämmtliche Divisoren δ von $p-1$ bezieht; wir wissen ferner schon, dass

$$\psi(\delta) \text{ entweder } = 0, \text{ oder } = \varphi(\delta)$$

ist. Da nun früher bewiesen ist (§. 13), dass auch

$$\Sigma \varphi(\delta) = p-1$$

ist, so folgt hieraus mit Nothwendigkeit, dass

$$\psi(\delta) \text{ niemals } = 0, \text{ sondern stets } = \varphi(\delta)$$

ist. Denn da jedes Glied $\psi(\delta)$ der erstern Summe dem entsprechenden der letztern höchstens gleich sein, aber niemals dasselbe übertreffen kann, so würde, sobald nur ein einziges Mal oder öfter $\psi(\delta) = 0$ wäre, die erstere Summe nothwendig kleiner ausfallen müssen als die letztere, während sie in der That einander gleich sind. Wir haben so den wichtigen Satz*) gewonnen:

Die Anzahl der sämmtlichen incongruenten Zahlen, welche zu einem bestimmten Divisor δ von $p-1$ gehören ist stets $= \varphi(\delta)$.

Es genügt, einen Blick auf das obige Beispiel zu werfen, in welchem $p = 7$, um diesen Satz bestätigt zu sehen.

§. 30.

Am interessantesten und folgenreichsten ist der in diesem Resultat enthaltene specielle Fall, in welchem $\delta = p-1$ ist:

Es giebt stets $\varphi(p-1)$ incongruente Zahlen g, welche zu dem Exponenten $p-1$ gehören, welche also die charakteristische Eigenschaft haben, dass die $p-1$ Potenzen

*) *Gauss: D. A.* art. 54.

$$1,\ g,\ g^2,\ g^3 \ldots g^{p-2} \qquad (G)$$

sämmtlich incongruent (mod. p) sind.

Da es überhaupt nur $p-1$ incongruente und durch p nicht theilbare Zahlen c giebt, so folgt, dass jede solche Zahl c einer, und natürlich auch nur einer der Potenzen (G) congruent ist. Jede solche Zahl g, welche zum Exponenten $p-1$ gehört, heisst eine *primitive Wurzel der Primzahl p**), und man kann daher sagen: wenn g eine primitive Wurzel von p ist, und c irgend eine durch p nicht theilbare Zahl, so existirt stets eine Zahl γ in der Reihe $0, 1, 2 \ldots p-2$ und nur eine von der Beschaffenheit, dass

$$c \equiv g^{\gamma} \pmod{p}$$

ist. Wenn man in dieser Weise alle incongruenten und — was im Folgenden immer hinzuzudenken ist — durch p nicht theilbaren Zahlen als Potenzen einer Basis g darstellt, so heissen die Exponenten γ die *Indices* der zugehörigen Zahlen c in Bezug auf die *Basis g*, und man schreibt z. B.

$$\text{Ind. } c = \gamma,$$

indem man die Basis g, so lange sie unverändert bleibt, in der Bezeichnung unterdrückt.

Nehmen wir z. B. $p = 13$, so überzeugt man sich leicht, dass 2 eine primitive Wurzel ist; denn durch Potenziren erhält man

$$2^0 \equiv 1,\quad 2^1 \equiv 2,\quad 2^2 \equiv 4,\quad 2^3 \equiv 8,\quad 2^4 \equiv 3,\quad 2^5 \equiv 6,$$
$$2^6 \equiv 12,\quad 2^7 \equiv 11,\quad 2^8 \equiv 9,\quad 2^9 \equiv 5,\quad 2^{10} \equiv 10,\quad 2^{11} \equiv 7.$$

Nehmen wir daher 2 zur Basis eines Systems von Indices, so erhalten wir folgende Tabellen

c	1	2	3	4	5	6	7	8	9	10	11	12
Ind. c	0	1	4	2	9	5	11	3	8	10	7	6

und

Ind. c	0	1	2	3	4	5	6	7	8	9	10	11
c	1	2	4	8	3	6	12	11	9	5	10	7

deren erstere dazu dient, zu einer Zahl c den Index zu finden, während die zweite den entgegengesetzten Zweck hat**).

Offenbar hat dieses ganze Verfahren die grösste Analogie mit

*) *Euler*: *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, Nov. Comm. Petrop. XVIII, p. 85.

**) Im *Canon Arithmeticus* von *Jacobi* (1839) findet man solche Tabellen für alle dem ersten Tausend angehörenden Primzahlen.

der Construction von Logarithmentafeln, die ja auf dem ähnlichen Gedanken beruhen, alle positiven Zahlen als Potenzen einer einzigen Basis darzustellen; und es zeigt sich nun auch, dass in der Zahlentheorie die Indices ähnliche Gesetze befolgen und für praktische Zwecke ebenso brauchbar sind, wie die Logarithmen. Zunächst leuchtet ein, dass zwei congruente Zahlen auch stets denselben Index haben, in Zeichen: wenn $a \equiv b \pmod{p}$, so ist auch $\text{Ind. } a = \text{Ind. } b$. Ist ferner $c \equiv ab \pmod{p}$, so ist $\text{Ind. } c \equiv \text{Ind. } a + \text{Ind. } b \pmod{p-1}$, oder kürzer, es ist stets

$$\text{Ind. } (ab) \equiv \text{Ind. } a + \text{Ind. } b \pmod{p-1}.$$

Denn es ist ja

$$a \equiv g^{\text{Ind.}a} \pmod{p}; \quad b \equiv g^{\text{Ind.}b} \pmod{p},$$

also

$$ab \equiv g^{\text{Ind.}a + \text{Ind.}b} \pmod{p};$$

nun ist aber auch

$$ab \equiv g^{\text{Ind.}(ab)} \pmod{p},$$

folglich

$$g^{\text{Ind.}(ab)} \equiv g^{\text{Ind.}a + \text{Ind.}b} \pmod{p}.$$

Da nun g eine primitive Wurzel von p, also eine zum Exponenten $\delta = (p-1)$ gehörende Zahl ist, so folgt aus §. 28 die Richtigkeit der zu beweisenden Congruenz nach dem Modul $p-1$. Nehmen wir unser obiges Beispiel, in welchem $p = 13$, so ist z. B.

$$\text{Ind. } (7) = 11, \quad \text{Ind. } (9) = 8,$$

folglich

$$\text{Ind. } (63) \equiv 19 \pmod{12}$$

oder

$$\text{Ind. } (63) = 7.$$

In der That ist aber $63 \equiv 11 \pmod{13}$, und $\text{Ind. } (11) = 7$. Man sieht aus diesem Beispiel, wie eine solche Doppeltafel der Indices dazu benutzt werden kann, mit Leichtigkeit die Classe (11) zu finden, welcher das Product (63) aus zwei Zahlen (7 und 9) angehört.

Natürlich lässt sich der vorstehende Satz auf ein Product aus beliebig vielen Factoren in folgender Weise ausdehnen:

$$\text{Ind. } (abc \ldots) \equiv \text{Ind. } a + \text{Ind. } b + \text{Ind. } c + \cdots \pmod{p-1}.$$

Nimmt man hierin alle Factoren einander congruent, so erhält man:

$$\text{Ind. } (a^n) \equiv n \text{ Ind. } a \pmod{p-1},$$

wo n irgend eine positive ganze Zahl bedeutet.

Es liesse sich hieraus auch leicht nachweisen, dass der Uebergang von einem System von Indices zu einem andern, dessen Basis eine andere der $\varphi(p-1)$ primitiven Wurzeln ist, ganz ähnlichen Gesetzen unterliegt, wie der Uebergang von einem Logarithmensystem zu einem andern; wir beschränken uns indessen auf folgende einfache Bemerkungen. Wie auch die Basis g gewählt sein mag, der Index von 1 ist stets $= 0$; denn es ist immer $g^0 = 1$. Ferner ist (den Fall $p = 2$ ausgenommen) der Index von -1 stets $= \frac{1}{2}(p-1)$; denn da nach §. 19

$$g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so muss mindestens eine der beiden Zahlen

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1$$

durch p theilbar sein; die erstere ist es aber nicht, denn sonst wäre

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

was mit der Voraussetzung im Widerspruch ist, dass g zum Exponenten $p-1$ gehört; es ist daher stets

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

und folglich

$$\text{Ind. } (-1) = \frac{p-1}{2}.$$

Es verdient endlich noch bemerkt zu werden, dass man die Indices, statt aus den Zahlen $0, 1, 2 \ldots (p-2)$, ebenso gut aus jedem andern vollständigen System incongruenter Zahlen in Bezug auf den Modul $p-1$ wählen kann; die so eben bewiesenen Fundamentalsätze erleiden dadurch nicht die geringste Aenderung.

Man kann nun die Indices benutzen, um eine Congruenz ersten Grades

$$ax \equiv b \pmod{p},$$

die hier die Stelle eines Divisionsproblems vertritt, mit Leichtigkeit aufzulösen; denn es muss offenbar

$$\text{Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1}$$

sein. Ist also z. B. die Congruenz

$$5x \equiv 6 \pmod{13}$$

zu lösen, so wird man, indem man wieder die primitive Wurzel 2 zur Basis des Indexsystems wählt,

$$\text{Ind. } x \equiv \text{Ind. } 6 - \text{Ind. } 5 \equiv 5 - 9 \equiv 8 \pmod{12}$$

und folglich

$$x \equiv 9 \pmod{13}$$

finden.

Diese Methode, Congruenzen ersten Grades aufzulösen, scheint auf den ersten Blick nur dann anwendbar, wenn der Modul eine Primzahl ist; allein man kann leicht zeigen, dass jede beliebige Congruenz ersten Grades

$$ax \equiv b \pmod{k},$$

deren Modul eine zusammengesetzte Zahl ist, auf eine Kette von Congruenzen reducirt werden kann, deren Moduln Primzahlen sind. Wir können uns hierbei auf den Fall beschränken, in welchem a relative Primzahl gegen k ist. Man löse nun zuerst die Congruenz

$$ax \equiv b \pmod{p},$$

wo p irgend eine in $k = pk'$ aufgehende Primzahl ist, nach der neuen Methode, so erhält man ein Resultat von der Form

$$x \equiv \alpha \pmod{p} \quad \text{oder} \quad x = \alpha + px',$$

wo x' eine beliebige ganze Zahl ist; substituirt man diesen Ausdruck in die gegebene Congruenz, so nimmt sie die folgende Form an:

$$pax' \equiv (b - a\alpha) \pmod{k}.$$

Da nun $b - a\alpha$ durch p theilbar, also von der Form $b'p$ ist, so stimmen sämmtliche Wurzeln der vorstehenden Congruenz mit den sämmtlichen Wurzeln der Congruenz

$$ax' \equiv b' \pmod{k'}$$

überein. Auf dieselbe Weise kann man nun fortfahren, indem man diese Congruenz zunächst nur in Bezug auf eine in k' aufgehende Primzahl p' löst, u. s. f.; man braucht dann zuletzt nur noch von der Wurzel der letzten dieser Congruenzen durch successive Substitution zu der der ursprünglichen überzugehen.

§. 31.

Wir benutzen nun noch die Theorie der Indices, um auf sie die Theorie der *binomischen Congruenzen* für einen Primzahl-

modulus p zu stützen; nach einer frühern Bemerkung kann man einer jeden solchen binomischen Congruenz die Form

$$x^n \equiv D \pmod{p} \tag{1}$$

geben, in welcher der Coefficient der Potenz der Unbekannten $= 1$ ist; da ferner der Fall, in welchem $D \equiv 0 \pmod{p}$ und folglich auch $x \equiv 0 \pmod{p}$, ohne Interesse ist, so schliessen wir denselben aus.

Bezeichnen wir nun zur Abkürzung die Indices von D und x resp. mit γ und ξ (wenn irgend eine primitive Wurzel g von p zur Basis genommen ist), so reducirt sich die Auflösung der Congruenz (1) auf die Bestimmung aller Wurzeln ξ der Congruenz ersten Grades

$$n\xi \equiv \gamma \pmod{p-1}; \tag{2}$$

denn offenbar entspricht jeder Wurzel der einen dieser beiden Congruenzen (1) und (2) auch stets eine und nur eine Wurzel der andern.

Es sei jetzt δ der grösste gemeinschaftliche Divisor der Zahlen $p-1$ und n, so ist (§. 22) die Congruenz (2) nur dann möglich, wenn die Bedingung

$$\gamma \equiv 0 \pmod{\delta} \tag{3}$$

erfüllt ist, und dann hat sie δ nach dem Modul $p-1$ incongruente Wurzeln ξ. Wir schliessen hieraus unmittelbar den Satz:

Ist δ der grösste gemeinschaftliche Divisor des Grades n der Congruenz (1) *und der Zahl $p-1$, so ist diese Congruenz nur dann möglich, wenn die Bedingung*

$$\text{Ind. } D \equiv 0 \pmod{\delta} \tag{4}$$

erfüllt ist, und dann besitzt sie δ nach dem Modul p incongruente Wurzeln x.

Liegt z. B. die Congruenz

$$x^8 \equiv 3 \pmod{13}$$

vor, so ist $\delta = 4$; nehmen wir ferner die primitive Wurzel 2 als Basis für die Indices, so ist Ind. $3 = 4$, also ist die Bedingung (4) erfüllt, und die vorgelegte Congruenz hat 4 nach dem Modul 13 incongruente Wurzeln; um diese zu finden, bilden wir die Congruenz ersten Grades

$$8\xi \equiv 4 \pmod{12} \quad \text{oder} \quad 2\xi \equiv 1 \pmod{3},$$

und erhalten hieraus

$$\xi \equiv 2 \pmod{3}$$

oder

$$\xi \equiv 2, \text{ oder } 5, \text{ oder } 8, \text{ oder } 11 \pmod{12},$$

folglich, indem wir zu diesen Indices ξ die zugehörigen Zahlen suchen,

$$x \equiv 4, \text{ oder } 6, \text{ oder } 9, \text{ oder } 7 \pmod{13}.$$

Da die Möglichkeit der binomischen Congruenz von der Wahl der primitiven Wurzel g, auf welche sich die Indices γ und ξ beziehen, nothwendig unabhängig sein muss, so wird das Kriterium, dass der Index γ einer Zahl D durch einen Divisor δ der Zahl $p-1$ theilbar sein muss, in eine von der Theorie der Indices unabhängige Form gebracht werden können. Dies bestätigt sich auf folgende Weise. Sobald in Bezug auf irgend eine Basis g der Index γ der Zahl D durch den Divisor δ von $p-1$ theilbar, also von der Form $h\delta$ ist, so haben wir die Congruenz

$$D \equiv g^{h\delta} \pmod{p}$$

und hieraus durch Potenzirung

$$D^{\frac{p-1}{\delta}} \equiv g^{h(p-1)} \equiv 1 \pmod{p};$$

und umgekehrt, sobald die Zahl D dieser Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$$

genügt, muss der in Bezug auf eine beliebige Basis g genommene Index γ der Zahl D durch δ theilbar sein; denn es sei

$$D \equiv g^{\gamma} \pmod{p},$$

so folgt hieraus

$$g^{\gamma \cdot \frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

und da g eine primitive Wurzel, d. h. eine zum Exponenten $p-1$ gehörende Zahl ist, so muss der Exponent durch $p-1$, und folglich der Index γ durch δ theilbar sein.

Nachdem das ursprüngliche Kriterium so umgeformt ist, können wir unsern Satz in folgender Weise unabhängig von der Theorie der Indices aussprechen:

Ist δ der grösste gemeinschaftliche Divisor der Zahlen n und $p-1$, so hat die Congruenz

$$x^n \equiv D \pmod{p}, \qquad (1)$$

genau δ incongruente Wurzeln, oder gar keine, je nachdem die Zahl D der Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p} \qquad (5)$$

genügt oder nicht genügt.

Den speciellen Fall, in welchem $\delta = n$ und $D = 1$ ist, haben wir schon früher (§. 27) auf anderm Wege bewiesen; es würde nicht schwer sein, aus den dort angewandten Principien auch den allgemeinen Satz abzuleiten, ohne die Theorie der Indices zu Hülfe zu rufen; doch überlassen wir der Kürze halber diese Untersuchung dem Leser.

Wir können nun auch noch die Frage aufstellen: wenn der Grad n der Congruenz (1) gegeben ist, wie viele incongruente Zahlen D existiren, für welche die Congruenz (1) möglich ist? Hierauf liefert der Satz selbst sogleich die Antwort, denn diese Zahlen D sind ja die sämmtlichen Wurzeln der binomischen Congruenz

$$x^{\frac{p-1}{\delta}} \equiv 1 \pmod{p};$$

der grösste gemeinschaftliche Divisor des Exponenten $(p-1):\delta$ und der Zahl $p-1$ ist in diesem Falle der Exponent $(p-1):\delta$ selbst, und da das Kriterium für die Möglichkeit offenbar erfüllt ist, so ist also die Anzahl aller incongruenten Zahlen D, für welche die Congruenz (1) möglich ist, genau $= (p-1):\delta$. Man nennt solche Zahlen D, welche einer $n$ten Potenz einer Zahl congruent sind, kurz $n$te Potenzreste, und wir können daher sagen:

Die Anzahl aller nten Potenzreste ist $= (p-1):\delta$, *wo* δ *den grössten gemeinschaftlichen Divisor der Zahlen* n *und* $p-1$ *bezeichnet.*

Man findet dieselben offenbar, wenn man alle incongruenten Zahlen zur $n$ten Potenz erhebt und deren Reste bildet. Wenn $n = 2, 3, 4$ ist, so nennt man diese Zahlen resp. *quadratische*, *cubische*, *biquadratische Reste.* Mit der Theorie der erstern, welche für sich allein schon eine grosse Ausdehnung besitzt, werden wir uns nun im Folgenden ausführlich beschäftigen.