Die Theorie der Reste, insbesondere derer vom dritten Grade,

nebst

einer Tafel der kubischen Reste aller Primzahlen der Form 6n + 1 zwischen den Grenzen 1 und 100.

Abschnitt I.

1.

Bezeichnet p hier, wie auch stets im Folgenden eine Primzahl und ist $p - 1 = nk$, so ist k die Anzahl der Reste vom Grade n.

Denn ist a Primitivwurzel, so sind die Reste der Potenzen $a^n, a^{2n}, \ldots a^{kn}$ sämmtlich von einander verschieden. Bezeichnet man dieselben mit r_1, r_2, r_k, so ist keine mit diesen incongruente Zahl der nten Potenz einer Zahl congruent.

Denn wäre r_{k+1} jeder der Grössen $r_1, r_2 \ldots$ incongruent, und gleichzeitig $r_{k+1} \equiv b^n$, so müsste $r_{k+1}^k \equiv b^{kn} \equiv 1$ sein, d. h. die Congruenz $x^k \equiv 1 Mp$ müsste die Wurzeln r_1, r_2, r_k, r_{k+1} haben, was unmöglich ist.

2.

Die Reste vom Grade n sind die Werthe des Ausdruckes $\sqrt[k]{1}\,Mp$.

Aus der Entstehung der Reste folgt, dass die kte Potenz eines jeden der Einheit congruent ist; daher enthält die Congruenz $x^k \equiv 1 Mp$ alle Reste vom Grade n als Wurzeln, Ferner ist $x^k - 1 \equiv (x - r_1)(x - r_2)(x - r_k)$. Entwickelt man die rechte Seite und vergleicht die Coefficienten gleicher Potenzen auf beiden Seiten, so ergiebt sich:

Die Summe der Combinationsformen der Reste — ohne Wiederholung — ist stets durch den Modul theilbar, ausgenommen die letzte Combinationsklasse oder das Product der Reste, das der positiven oder negativen Einheit congruent ist, je nachdem ihre Anzahl ungerade oder gerade ist.

Universitäts- und
Landesbibliothek Düsseldorf

Ebenso sind alle Nichtreste vom Grade n die Wurzeln der Congruenz $\frac{x^{nk}-1}{x^k-1} \equiv 0$, oder nach Ausführung der Division die Wurzeln von $x^{k(n-1)} + x^{k(n-2)} \ldots + x^k + 1 \equiv 0$.

Hieraus folgt unter Anderem, dass die Summe der Nichtreste, falls n von 2 verschieden, durch den Modul theilbar und dass ihr Product der positiven oder negativen Einheit congruent ist, je nachdem ihre Zahl gerade oder ungerade.

Auch würde es leicht sein, die Sätze, welche sich auf die übrigen Combinationsklassen beziehen, in Worte zu fassen.

Hiernach lassen sich die Zahlen von 1 bis $p-1$ in k Gruppen zerlegen, die je n Glieder enthalten, wenn man die Wurzeln derselben Congruenz vom nten Grade jedesmal zu einer Gruppe zusammenfasst. Anders ausgedrückt heisst dies, dass jeder der Ausdrücke: $\sqrt[n]{r_1}, \sqrt[n]{r_2}, \ldots \sqrt[n]{r_k}$ n von einander verschiedene Werthe besitzt und dass jeder Werth eines Ausdrucks jedem Werthe eines andern Ausdrucks incongruent ist.

3.

Ist die Primzahl n kleiner als p und Nichttheiler von $p-1$, so ist jede der Zahlen von 1 bis $p-1$ Rest vom Grade n.

Denn bedeutet a, eine Primitivwurzel für den Modul p, so sind die Reste der Potenzen $a^n, a^{2n}, \ldots a^{(p-1)n}$ sämmtlich incongruent, gleichwie die Reste von $a, a^2, \ldots a^{p-1}$.

Beisp. $\sqrt[3]{1}, \sqrt[3]{2}, \ldots \sqrt[3]{10}$ M11 sind stets einwerthig, ebenso wie $\sqrt[3]{1}, \sqrt[3]{2}, \ldots \sqrt[3]{22}$ M23. Anders ausgedrückt lautet der Satz:

Ist n prim gegen p, kleiner als p und Nichttheiler von $p-1$, so ist p stets Theiler von $x^n - A$, wenn A eine beliebige positive oder negative, durch p nicht theilbare, ganze Zahl bedeutet.

4.

Beziehung der Primitivwurzeln zu den Resten.

Ist $p-1 = a^\alpha b^\beta c^\gamma \ldots$, wo a, b, c verschiedene Primzahlen, sondert man ferner von den Zahlen von 1 bis $p-1$ alle Reste ab, die den Graden a, b, c angehören, so bleiben sämmtliche Primitivwurzeln zurück.

Beweis. Die Reste vom Grade a sind die Wurzeln von $x^{a^{\alpha-1} b^\beta c^\gamma} \equiv 1$.

» » » » b » » » » $x^{a^\alpha b^{\beta-1} c^\gamma} \equiv 1$.

» » » » c » » » » $x^{a^\alpha b^\beta c^{\gamma-1}} \equiv 1$.

Jede Zahl A, die keiner dieser Congruenzen genügt, gehört zum Exponenten $p-1$, ist mithin Primitivwurzel.

Denn gehörte sie zu einem Theile von $p-1$, so ist derselbe von der Form $a^{\alpha_1} b^{\beta_1} c^{\alpha_1}$, wo $\alpha_1, \beta_1, \gamma_1$, nicht gleichzeitig mit α, β, γ übereinstimmen; dann müsste aber A einer von jenen drei Congruenzen genügen, was der Voraussetzung widerstreitet.

Universitäts- und
Landesbibliothek Düsseldorf

Beisp. Ist $p = 13$, so sind
die quadratischen Reste: 1, 3, 4, 9, 10, 12,
die kubischen Reste: 1, 5, 8, 12,
die Primitivwurzeln: 2, 6, 7, 11.
Zur Probe dient, dass $2 + 6 + 7 + 11 \equiv 0 M 13$.

Ist $p = 17$, so sind
die quadratischen Reste: 1, 2, 4, 8, 9, 13, 15, 16,
also die Primitivwurzeln: 3, 5, 6, 7, 10, 11, 12, 14.
Bezeichnet man die Summe der Primitivwurzeln durch ΣP, so ist $\Sigma P \equiv 0 M 17$.

Ist $p = 19$, so sind
die quadratischen Reste: 1, 4, 5, 6, 7, 9, 11, 16, 17,
die kubischen Reste: 1, 7, 8, 11, 12, 18,
die Primitivwurzeln: 2, 3, 10, 13, 14, 15.
Auch ist $\Sigma P = 57 \equiv 0 M 19$.

Ist $p = 23$, so sind
die Reste vom 2ten Grade: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
» » » 11ten » : 1, 22,
also die Primitivwurzeln: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.
Auch ist $\Sigma P = 139 \equiv 1 M 23$.

Ist $p = 29$, so sind
die Reste vom 2ten Grade: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28,
» » » 7ten » : 1, 12, 17, 28,
also die Primitivwurzeln: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.
Auch ist $\Sigma P = 174 \equiv 0 M 29$.

Ist $p = 31$, so sind
die Reste vom 2ten Grade: 1, 2, 4, 7, 8, 9, 10, 14, 16, 18, 19, 20, 28, 30,
» » » 3ten » : 1, 2, 4, 8, 15, 16, 23, 27, 29, 30.
» » » 5ten » : 1, 5, 6, 25, 26, 30,
also die Primitivwurzeln: 3, 11, 12, 13, 17, 21, 22, 24.
Auch ist $\Sigma P = 123 \equiv -1 M 31$.

Zur Ermittelung der Primitivwurzeln der Primzahlen 37, 73, 97 würden die Tafeln der quadratischen und kubischen Reste völlig ausreichen.

5.

Die entwickelten Formen der Congruenzen, welche nur Primitivwurzeln zu Wurzeln haben.

Die Bezeichnung „Primitivwurzel“ hat einen weitern und engern Sinn. Ist $a^d \equiv 1 Mp$, während die tiefern Potenzen von a der Einheit nicht congruent sind, so heisst a Primitivwurzel für den Exponenten d nach dem Modul p.

Diejenigen Zahlen, welche zum Exponenten $p - 1$ gehören, heissen Primitivwurzeln im engern Sinne.

Universitäts- und
Landesbibliothek Düsseldorf

Die Congruenzen der Primitivwurzeln für die Exponenten 1 bis 21 sind folgende:

1) $x - 1 \equiv 0.$
2) $x + 1 \equiv 0.$
3) $x^2 + x + 1 \equiv 0.$
4) $x^2 + 1 \equiv 0.$
5) $x^4 + x^3 + x^2 + x + 1 \equiv 0.$
6) $x^2 - x + 1 \equiv 0.$
7) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0.$
8) $x^4 + 1 \equiv 0.$
9) $x^6 + x^3 + 1 \equiv 0.$
10) $x^4 - x^3 + x^2 - x + 1 \equiv 0.$
11) $x^{10} + x^9 + \ldots + x + 1 \equiv 0.$
12) $x^4 + x^2 + 1 \equiv 0.$
13) $x^{12} + x^{11} + \ldots + x + 1 \equiv 0.$
14) $x^6 + x^5 + x^4 - x^3 + x^2 - x + 1 \equiv 0.$
15) $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \equiv 0.$
16) $x^8 + 1 \equiv 0.$
17) $x^{16} + x^{15} + \ldots + x + 1 \equiv 0.$
18) $x^6 - x^3 + 1 \equiv 0.$
19) $x^{18} + x^{17} + \ldots + x + 1 \equiv 0.$
20) $x^8 - x^6 + x^4 - x^2 + 1 \equiv 0.$
21) $x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1 \equiv 0.$

Ist etwa 6 Theiler von $p - 1$, so enthält die Congruenz $x^2 - x + 1 \equiv 0$ stets die zwei Zahlen zu Wurzeln, die zum Exponenten 6 gehören. So gehören zum Exponenten 6 nach dem Modul 13 die zwei Zahlen 4 und 10; mithin hat man

$$4^2 - 4 + 1 \equiv 0 \text{M} 13,$$
$$10^2 - 10 + 1 \equiv 0.$$

Ebenso gehören zum Exponenten 6 nach dem Modul 19 die zwei Zahlen 8 und 12; mithin hat man

$$8^2 - 8 + 1 \equiv 0 \text{M} 19,$$
$$12^2 - 12 + 1 \equiv 0.$$

Man bemerkt leicht, dass die Coefficienten der Glieder der entwickelten Congruenzen entweder ± 1 oder 0 sind. Sind ferner 2 Exponenten der Form $a^\alpha b^\beta c^\gamma, \ldots$ und $2 . a^\alpha . b^\beta c^\gamma \ldots$, wo a, b, c verschiedene ungerade Primzahlen vorstellen, so unterscheidet sich die Congruenz des ersten Exponenten von der des zweiten nur durch die Vorzeichen der Glieder grader Stelle. Die Wahrheit dieser Angabe ergiebt sich durch Vergleichung der Congruenzen 3) und 6), 5) und 10), 7) und 14), 9) und 18), auch lässt sich erweisen, dass diese Beziehung ganz allgemein stattfindet. Denn gehört g zum Exponenten $a^\alpha b^\beta c^\gamma$, so gehört $-g$ zum Exponenten $2 . a^\alpha b^\beta c^\gamma$, da ja die einzige Zahl, die zum Exponenten 2 gehört, die negative Einheit ist. Daraus folgt, dass die Wurzeln der zweiten Congruenz aus denen der ersten lediglich durch Aenderung der Vorzeichen erhalten werden; natürlich kann man durch dieselbe Aenderung von den Wurzeln der zweiten Congruenz zu denen der erstern übergehen.

Beisp. Für den Modul 19 gehören zum Exponenten 3 die Zahlen 7, 11; zum Exponenten 6 die Zahlen 8, 12. Nun ist $7 \equiv -12 \text{M} 19$,
$11 \equiv -8.$

Für denselben Modul gehören zum Exponenten 9 die Zahlen 4, 5, 6, 9, 16, 17; zum Exponenten 18 die Zahlen 2, 3, 10, 13, 14, 15. Nun ist

$4 \equiv -15,$ $6 \equiv -13,$ $16 \equiv -3,$
$5 \equiv -14,$ $9 \equiv -10,$ $17 \equiv -2.$

Dieser Satz lässt sich bei der Entwickelung der Congruenzen häufig mit Vortheil anwenden.

Ist etwa der Exponent von der Form $a . b . c$, wo a, b, c ungleiche Primzahlen, so ist die Congruenz, welche zum Exponenten $a . b . c$ gehört, in unentwickelter Form:

Universitäts- und
Landesbibliothek Düsseldorf

$$\frac{(x^{abc}-1)\,x^{a}-1)\,(x^{b}-1)\,(x^{c}-1)}{(x-1)\,(x^{ab}-1)\,(x^{ac}-1)\,(x^{bc}-1)}\equiv 0.$$

Die linke Seite ist eine ganze Function vom Grade $(a-1)(b-1)(c-1)$; jedoch würde die Entwickelung der Producte und die Ausführung der Division umständlich sein.

Für $abc = 30$, geht die letzte Congruenz über in:

$$\frac{(x^{30}-1)\,(x^{2}-1)\,(x^{3}-1)\,(x^{5}-1)}{(x-1)\,(x^{6}-1)\,(x^{10}-1)\,(x^{15}-1)}\equiv 0.$$

Die entwickelte Form dieser Congruenz lässt sich jedoch leichter aus derjenigen herleiten, welche oben für den Exponenten 15) aufgestellt worden ist. Unter Anwendung des oben erwiesenen Satzes ergiebt sich dieselbe: $x^{8}+x^{7}-x^{5}-x^{4}-x^{3}+x+1\equiv 0$.

Ist also $30n+1$ eine Primzahl, so hat die Congruenz

$$x^{8}+x^{7}-x^{5}-x^{4}-x^{3}+1\equiv 1\,M(30n+1)$$

stets 8 von einander verschiedene reelle Wurzeln.

Im Falle, dass der Exponent die Potenz einer Primzahl, etwa a^{k}, lässt sich die zugehörige Congruenz in entwickelter Form a priori bestimmen. Denn die Zahlen, welche zum Exponenten a^{k} gehören, genügen der Congruenz $\frac{x^{a^{k}}-1}{x^{a^{k-1}}-1}\equiv 0$, woraus man durch Division erhält:

$$x^{a^{k-1}(a-1)}+x^{a^{k-1}(a-2)}+x^{a^{k-1}(a-3)}+\ldots\ldots+x^{a^{k-1}}+1\equiv 0.$$

Was aber den oben aufgestellten Congruenzen besonderes Interesse verleiht, ist, dass die Auflösung einer jeden auf die Lösung einer Anzahl binomischer Congruenzen, d. h. soweit die Indextafel reicht, auf die Auflösung einer Anzahl linearer Congruenzen zurückgeführt werden kann.

Die Gauss'sche Indextafel ist hierzu nur theilweise geeignet, da man durch dieselben für die Primmoduln von 1 bis 97 zwar für jede Zahl unterhalb des Moduls den zugehörigen Index, aber nicht umgekehrt für jeden Index unterhalb des Moduls die zugehörige Zahl findet. Die letztere Operation wird aber sehr erleichtert, wenn man für jeden Primmodul die kleinste Primitivwurzel wählt, was Gauss aus andern Gründen nicht gethan hat.

Wählt man für den Primmodul 31 die kleinste Primitivwurzel 3 zur Basis, so entsprechen den Indices:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 —
3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1.

als zugehörige Zahlen.

Die Auflösung der Congruenz $x^{4}-x^{3}+x^{2}-x+1\equiv 0M31$, die zum Exponenten 10) gehört, würde nach dem Obigen vermittelt durch Auflösung der Congruenzen

$$x^{10}\equiv 1\,M31,\qquad x^{5}\equiv 1,\qquad x^{2}\equiv 1,\qquad x^{1}\equiv 1.$$

Zuletzt hat man die Wurzeln der drei letzten Congruenzen von denen der ersten fortzulassen, wobei natürlich eine simultane Wurzel mehrer Congruenzen nur einmal gezählt wird. Noch einfacher ist es, die Zahlen, welche zu den Exponenten 1, 2, 5 gehören, fafls jene schon bekannt sind, fortzulassen.

Universitäts- und
Landesbibliothek Düsseldorf

Nun folgt aus

$$x^{10} \equiv 1 M 31,$$
$$10 \operatorname{Ind} x \equiv 0 M 30,$$
$$\operatorname{Ind} x = 0, 3, 6, 9, 12, 15, 18, 21, 24, 27 \text{ und}$$
$$x \equiv 1, 27, 16, 29, 8, 30, 4, 15, 2, 23.$$

Lässt man hiervon diejenigen Zahlen fort, die zu den Exponenten 1, 2, 5 gehören, nämlich die Zahlen: 1, 30, 2, 4, 8, 16, so sind 15, 23, 27, 29 die Wurzeln von

$$x^4 - x^3 + x^2 - x + 1 \equiv 0 M 31.$$

Durch eine ähnliche Rechnung ergeben sich die Wurzeln der Congruenzen 1) 2) 3) 5) 6) 10) 15) für den Modul 31, nämlich für:

1) 1,	6) 6, 26,
2) 30,	10) 15, 23, 27, 29,
3) 5, 25,	15) 7, 9, 10, 14, 18, 19, 20, 28.
4) 2, 4, 8, 16,	

Abschnitt II.

Die reinen Congruenzen vom dritten Grade.

1.

Ist $x^3 \equiv AMp$, so heisst A kubischer Rest für den Modul p; p bedeutet im Folgenden stets eine Primzahl.

Ist p von der Form $3m + 2$, so lassen die dritten Potenzen der Zahlen von 1 bis $p-1$ lauter verschiedene Reste. Denn ist a Primitivwurzel für den Modul p, so hat man die Congruenzen

$$a^1 \equiv \alpha_1,$$
$$a^2 \equiv \alpha_2,$$
$$\vdots \quad \vdots \quad \vdots$$
$$a^{p-1} \equiv \alpha_{p-1},$$

worin die rechten Seiten sämmtliche Zahlen von 1 bis $p-1$ in irgend einer Reihenfolge enthalten. Wären nun 2 dritte Potenzen der Reste $\alpha_1, \alpha_2 \ldots$ einander congruent, etwa $\alpha_r^3 \equiv \alpha_s^3$, während $r > s$, so müsste $a^{3(r-s)} \equiv 1$ sein; hieraus würde $3(r-s) \equiv 0 Mp-1$ folgen, was unmöglich ist.

2.

Ist p von der Form $3m + 1$, so ist die Anzahl der kubischen Reste $\frac{1}{3}(p-1)$, die der Nichtreste $\frac{2}{3}(p-1)$. Der Beweis beruht darauf, dass der Index eines kubischen Restes stets durch 3 theilbar, während gleichzeitig die Anzahl der durch 3 theilbaren Zahlen in der Zahlenreihe von 1 bis $p-1$ gleich $\frac{p-1}{3}$ ist.

Hieraus folgt, dass die Congruenz $x^3 \equiv AMp$ drei reelle Wurzeln besitzt oder keine, je nachdem A kubischer Rest oder Nichtrest ist.

Universitäts- und
Landesbibliothek Düsseldorf

3.

Berechnung der kubischen Reste.

Am Ende der Abhandlung befindet sich eine Tafel der kubischen Reste für die Primzahlen der Form $6m + 1$ von 1 bis 97. Für die Ermittelung dieser Reste lässt sich bisweilen die Indextafel mit Vortheil verwenden. Falls jedoch die Primitivwurzel für den betreffenden Modul 2 oder 10 ist, so thut man am Besten, die kleinsten positiven Reste der Potenzen $2^3, 2^6, 2^9, \ldots 2^{p-1}$ oder $10^3, 10^6, \ldots 10^{p-1}$ direct zu suchen.

4.

Die kubischen Reste der Potenzen von Primzahlen.

Ist p von 3 verschieden, so ist jeder Rest von p^n, der gegen p prim, auch Rest für p^{n+1}. Denn sei 1) $a^3 \equiv rMp^n$, und setzt man

2) $y^3 \equiv rMp^{n+1}$, so ist $y^3 \equiv a^3Mp^n$. Sei $y = a + xp^n$, so ist

3) $a^3 + 3a^2xp^n + 3ax^2p^{2n} \equiv rMp^{n+1}$ oder

4) $\frac{a^3 - r}{p^n} + 3a^2x \equiv 0Mp.$

Diese Congruenz liefert stets einen Werth für x, da $3a^2$ gegen p prim ist.

5.

Ist p von der Form $3m + 2$ und r prim gegen p, so hat der Ausdruck $\sqrt[3]{rMp^{n+1}}$ stets einen einzigen reellen Werth und jede Primzahl gegen p, die unterhalb p^{n+1} liegt, ist ein kubischer Rest für den Modul p^{n+1}.

Denn besitzt die Congruenz $x^3 \equiv rMp^n$ nur eine Wurzel, so besitzt dieselbe Congruenz nach dem Modul p^{n+1} auch nur eine Wurzel.

Wäre andernfalls
$$a^3 \equiv rMp^{n+1},$$
$$b^3 \equiv r,$$
worin a und $b < p^{n+1}$, so müssten dieselben Congruenzen für den Modul p^n bestehen, also wenn α und β die kleinsten positiven Reste von a und b für den Modul p^n bedeuten:
$$\alpha^3 \equiv rMp^n,$$
$$\beta^3 \equiv r,$$
was der Annahme widerstreitet, falls α von β verschieden. Hieraus folgt zunächst, dass die kleinsten positiven Reste von a und b, nach dem Modul p^n, identisch sind und daher $a \equiv bMp^n$ sein muss. Setzt man daher $b = a + xp^n$, worin x irgend eine ganze Zahl zwischen 0 und $p-1$, so ist
$$a^3 \equiv a^3 + 3a^2xp^n + 3ax^2p^{2n} + p^{3n}Mp^{n+1},$$
$$3a^2x \equiv 0Mp,$$
$$x = 0.$$

Nun besitzt die Congruenz $x^3 \equiv rMp$ nur eine einzige Wurzel; mithin gilt dieselbe Behauptung von derselben Congruenz für jeden Modul, der eine Potenz von p ist. Aus dem Obigen folgt noch, dass die Wurzel der Congruenz $x^3 \equiv rMp^{n+1}$ in dem Intervall von p^n bis p^{n+1} liegt, falls sie von der Wurzel der Congruenz $x^3 \equiv rMp^n$ verschieden ist.

Universitäts- und
Landesbibliothek Düsseldorf

6.

Aus dem vorigen Paragraphen folgt, dass für den Modul 2^n alle ungeraden Zahlen unterhalb 2^n kubische Reste sind.

Ferner ist $(2^{n-1} \pm 1)^3 \equiv 2^{n-1} \pm 1 M 2^n$; denn

$$\begin{aligned}(2^{n-1} \pm 1)^3 &= 2^{3(n-1)} \pm 3 \,.\, 2^{2(n-1)} + 3 \,.\, 2^{n-1} \pm 1,\\ &\equiv 3 \,.\, 2^{n-1} \pm 1 M 2^n,\\ &\equiv 2^n + 2^{n-1} \pm 1,\\ &\equiv 2^{n-1} \pm 1.\end{aligned}$$

Hieraus folgt z. B. $7^3 \equiv 7 M 16$, $15^3 \equiv 15 M 32$,
$9^3 \equiv 9$ $\quad 17^3 \equiv 17$.

Auch sieht man leicht, dass die Reste der dritten Potenzen der ungeraden Zahlen stets der Klasse $4n + 1$ oder $4n + 3$ angehören, je nachdem ihre Zahlen der einen oder der andern Klasse angehören.

7.

Ist p von der Form $3m + 1$, so ist die Anzahl der Reste für den Modul p^n, welche Primzahlen gegen p sind, gleich $\frac{1}{3} p^{n-1}(p-1)$ und die Anzahl der Nichtreste gleich $\frac{2}{3} p^{n-1}(p-1)$.

Denn besitzt die Congruenz 1) $y^3 \equiv r M p^n$ drei von einander verschiedene Wurzeln, die kleiner sind als p^n, so besitzt 2) $y^3 \equiv r M p^{n+1}$ ebenfalls drei von einander verschiedene Wurzeln, die kleiner sind als p^{n+1}. Sind a, b, c die Wurzeln von 1), so sind $a + x_1 p^n$, $b + x_2 p^n$, $c + x_3 p^n$, worin x_1, x_2, x_3 kleiner als p, die drei Wurzeln von 2). Ferner sind die 3 letzten Wurzeln von einander verschieden. Denn wäre etwa $a + x_1 p^n = b + x_2 p^n$, so müsste $a \equiv b M p^n$ sein, was der Voraussetzung widerstreitet.

Wäre nun d eine vierte Wurzel von 2, kleiner als p^{n+1} und von den 3 vorigen verschieden, so müsste sie in dem Intervall von p^n bis p^{n+1} liegen. Da sie ferner der Congruenz 1) genügt, so müsste sie einer der Formen $a + xp^n$, $b + xp^n$, $c + xp^n$ angehören und x muss kleiner als p sein. Im erstern Falle wäre $(a + xp^n)^3 \equiv r M p^{n+1}$, oder $\frac{a^3 - r}{p^n} + 3a^2 x \equiv 0 M p$. Aus dieser Congruenz wird aber (§. 4) der Werth von x_1 bestimmt, woraus folgt, dass die Congruenz $x^3 \equiv r M p^{n+1}$ nur drei Wurzeln besitzt.

8.

Kubische Reste für die Potenzen von 3.

Ist r prim gegen 3, kleiner als 3^n und kubischer Rest für 3^n, so ist r auch kubischer Rest für 3^{n+1}, falls $n \geqq 2$.

Beweis. Ist $a^3 \equiv r M 3^n$, so wird eine Wurzel von $y^3 \equiv r M 3^{n+1}$ auf folgende Weise gefunden:

Man setze $y = a + x \,.\, 3^{n-1}$, so ist $\frac{a^3 - r}{3^n} + a^2 x \equiv 0 M 3$. Da a gegen 3 prim, so liefert diese Congruenz stets einen Werth für x.

Die kubischen Reste für den Modul 3 sind 1, 2, die für den Modul 9 sind 1, 8. Hieraus folgt, dass für den Modul 3^n alle Zahlen, die kleiner als 3^n und einer der Formen

Universitäts- und
Landesbibliothek Düsseldorf

$1 + 9n$, oder $8 + 9n$ angehören, kubische Rest sind; auch sieht man leicht, dass es ausser den Zahlen, die einer dieser beiden Klassen angehören, keine kubischen Reste für den Modul 3^n giebt.

Daher ist für $n > 2$ die Anzahl der kubischen Reste für den Modul 3^n gleich $2 . 3^{n-2}$, die der Nichtreste gleich $4 . 3^{n-2}$; woraus ersichtlich, dass bezüglich der Anzahl der Reste und Nichtreste für die Potenzen von 3 dasselbe Gesetz gilt, wie für die Potenzen der Primzahlen der Form $3m + 1$.

Noch ist zu erweisen, dass keine Congruenz mehr wie 3 Wurzeln hat. Denn sind $r_1, r_2, r_3 \ldots . r_m$ sämmtliche kubische Reste, die prim gegen 3 und kleiner als 3^n, so besitzt jede Gongruenz 1) $x^3 \equiv r, M 3^n$ drei Wurzeln, da jede dieser Congruenzen nach dem Modul 9 stets 3 Wurzeln hat. Hätte die Congruenz 1) eine vierte Wurzel δ, so würde eine Congruenz, etwa 2) $x^3 \equiv r_m M 3^n$ entweder nur 2 Wurzeln haben, oder δ würde den Congruenzen 1) und 2) gleichzeitig genügen. Dann wäre aber $r_m \equiv r, M 3^n$, was nicht angeht.

9.

Beziehung zwischen den kubischen Resten einer Zahl und den kubischen Resten ihrer Factoren.

Ist $m = a . b . c$ und a, b, c ungleiche Primzahlen oder Potenzen derselben; ist ferner rRm, so ist rRa, rRb, rRc. Ist rNa, so ist rNm.

Ferner wenn rRa,
rRb,
rRc, so ist rRm,

Denn sei $A^3 \equiv rMa$,
$B^3 \equiv rMb$,
$C^3 \equiv rMc$ und ist D diejenige Zahl, die nach den Moduln a, b, c die Reste A, B, C lässt, so ist $D^3 \equiv rMm$.

Beispiel: $4^3 \equiv 12M13$,
$10^3 \equiv 12M19$.

Setzt man $x \equiv 4M13$,
$x \equiv 10M19$,

$x \equiv 238M13 . 19$,

also $238^3 \equiv 12M13 . 19$.

Auch sieht man leicht, dass die Congruenz $x^3 \equiv 12M13 . 19$ 9 verschiedene Wurzeln besitzt, da jede der Congruenzen $x^3 \equiv 12M13$ und $x^3 \equiv 13M19$ deren 3 hat.

10.

Merkmale der kubischen Reste von p^n, wenn die Reste durch p theilbar sind:

1) Ist $k \geq n$ und a prim gegen p, so ist ap^k stets Rest.
2) Ist $k < n$, so ist ap^k Nichtrest, falls k durch 3 untheilbar ist. Ist k durch 3 theilbar, so ist ap^k kubischer Rest oder Nichtrest für den Modul p^n, je nachdem a kubischer Rest oder Nichtrest für p ist.

Universitäts- und
Landesbibliothek Düsseldorf

Der Beweis lässt sich leicht finden, soll daher der Kürze wegen hier übergangen werden.

11.

Die Anzahl der Werthe des Ausdrucks $\sqrt[3]{A}Mp^n$, falls A durch p theilbar ist.

Ist 1) $x^3 \equiv AMp^n$, $A = ap^{3\mu}$, a kubischer Rest für p und $n > 3\mu$, setzt man ferner $V = \sqrt[3]{A}Mp^n$ und $V_1 = \sqrt[3]{a}Mp^{n-3\mu}$ und ist v irgend ein Werth des letztern Ausdrucks, so genügen der Congruenz 1) die Producte von p^μ mit den Gliedern der Reihe v, $v + p^{n-3\mu}$, $v + 2p^{n-3\mu}, \ldots . v + (p^{2\mu} - 1)\, p^{n-3\mu}$.

Diese Producte

$$vp^\mu,\ vp^\mu + p^{n-2\mu},\ vp^\mu + 2p^{n-2\mu}, \ldots . vp^\mu + (p^{2\mu} - 1)\, p^{n-2\mu}$$

sind nach dem Modul p^n sämmtlich incongruent. Hieraus folgt, dass die Anzahl der Wurzeln von 1) entweder $p^{2\mu}$ oder $3p^{2\mu}$ beträgt, je nachdem der Ausdruck $\sqrt[3]{a}Mp^{n-3\mu}$ einen oder 3 Werthe hat.

Ist zweitens $n = 3\mu$, so hat die Congruenz 1) die Wurzeln o, p^μ, $2p^\mu, \ldots . (p^{2\mu} - 1)p^\mu$, welche sämmtlich für den Modul p^n incongruent sind.

12.

Für die Zahlen, die kleiner als der Primmodul p, gelten folgende Sätze:

Die kubischen Reste sind paarweise complementär, desgleichen die kubischen Nichtreste. Denn ist $a^3 \equiv r$, so ist $-a^3 \equiv -r$ oder $(p-a)^3 \equiv p - r$. Hieraus folgt ferner, dass $+n$ und $-n$ gleichzeitig kubische Nichtreste sind. Wäre nämlich $b^3 \equiv -n$, so müsste auch $(-b)^3 \equiv n$, also n Rest sein.

13.

Das Product zweier kubischer Reste ist stets ein kubischer Rest; das Product eines Restes mit einem Nichtreste stets Nichtrest.

Der erste Theil des Satzes ergiebt sich von selbst. Zum Beweis des andern Theils seien $r_1, r_2, \ldots r_k$ sämmtliche Reste unterhalb p, p selbst von der Form $6m + 1$, ferner seien $n_1, n_2, \ldots n_{2k}$ sämmtliche Nichtreste. Bildet man die Producte r_1^2, $r_1 r_2, \ldots . r_1 r_k$; dieselben sind einander incongruent, müssen daher die Zahlen $r_1, r_2, \ldots r_k$ zu linearen Resten haben. Hieraus folgt, dass $r_1 x \equiv r_2$ nur durch einen kubischen Rest auflösbar, oder dass $\frac{r_2}{r_1}Mp$ stets kubischer Rest ist. Also muss das Product eines Restes mit einem Nichtreste ein Nichtrest sein.

Das Quadrat eines kubischen Nichtrestes ist stets Nichtrest. Denn ist n ein Nichtrest, so hat man $n^3 \equiv n \,.\, n^2$; die linke Seite ist kubischer Rest, während der erste Factor rechter Hand Nichtrest ist, also muss der zweite Factor n^2 ebenfalls ein Nichtrest sein.

14.

Beziehung der Wurzeln einer kubischen Congruenz zu den quadratischen Resten und Nichtresten.

Universitäts- und
Landesbibliothek Düsseldorf

Sind a und $b < p$, p von der Form $6m + 1$ und ist $a^3 \equiv b^3$, so sind a und b gleichzeitig quadratische Reste oder Nichtreste.

Denn aus $a^3 \equiv b^3 Mp$ folgt $(a - b)(a^2 + ab + b^2) \equiv 0$ oder $(a + b)^2 \equiv ab$.

Sind also a, b, c die 3 Wurzeln von $x^3 \equiv r$, so hat man $a^3 \equiv b^3 \equiv c^3$ und die Producte ab, ac, bc müssen gleichzeitig quadratische Reste sein, woraus die Behauptung erhellt.

Beispiel: $\sqrt[3]{1} M7 = 1, 2, 4$ 1, 2, 4 sind quadratische Reste,

$\sqrt[3]{3} M7 = 3, 5, 6$ 3, 5, 6 sind quadratische Nichtreste,

$\sqrt[3]{8} M13 = 2, 5, 6$ 2, 5, 6 sind quadratische Nichtreste,

$\sqrt[3]{12} M13 = 4, 10, 12$ 4, 10, 12 sind quadratische Reste.

15.

Auflösung der Congruenz $ax^3 \equiv b$.

Ist $p = 3m + 1$, so ist die Bedingung für das Vorhandensein von Wurzeln, dass a und b gleichzeitig kubische Reste oder Nichtreste sind. Denn aus der obigen Congruenz folgt $a^3x^3 \equiv a^2b$, d. h. a^2b muss kubischer Rest sein, was nur eintritt, wenn a und b gleichzeitig kubische Reste oder Nichtreste sind.

Ist in diesem Falle $\alpha^3 \equiv \beta^3 \equiv \gamma^3 \equiv a^2b$, so sind $\frac{\alpha}{a} Mp$, $\frac{\beta}{a} Mp$, $\frac{\gamma}{a} Mp$ sämmtlich Wurzeln von $ax^3 \equiv b$. Ausser diesen dreien hat die Congruenz keine Wurzeln.

Beispiel: $5x^3 \equiv 8 M13$,

$125x^3 \equiv 200 \equiv 5$,

$7^3 \equiv 8^3 \equiv 11^3 \equiv 5$.

Also sind $\frac{7}{5} M13$, $\frac{8}{5} M13$, $\frac{11}{5} M13$ oder 4, 12, 10 die Wurzeln von $5x^3 \equiv 8$.

16.

Die Congruenz $x^3 \equiv r Mm$, wo $m = a . b . c \ldots\ldots$, während die Factoren von m entweder 2 oder 3, oder Primzahlen der Form $6n + 5$ sind, ist stets lösbar und hat eine einzige reelle Wurzel, wenn r prim gegen m.

Der Beweis folgt aus 9, Abschnitt II.

Beispiel: Es sei zu lösen $x^3 \equiv 5 M 2 . 3 . 11$. Nun ist

$1^3 \equiv 1 M2$,

$2^3 \equiv 2 M3$,

$3^3 \equiv 5 M11$.

Die Zahl, welche nach den Moduln 2, 3, 11 die Reste 1, 2, 5 lässt, ist 47, folglich $47^3 \equiv 5 M66$.

17.

Die Congruenz $x^3 \equiv r Mm$, ist gleichfalls lösbar und besitzt eine reelle Wurzel, wenn die Factoren von m Potenzen von Primzahlen der Form $6n + 5$ sind, während r prim gegen p.

Der Beweis folgt aus Abschnitt II. §. 5 und 9.

Universitäts- und
Landesbibliothek Düsseldorf

18.

Ist p von der Form $6m + 1$, so ist jeder kubischer Rest der dritten Potenz einer Zahl congruent, die $\frac{2}{3}(p-1)$ nicht übersteigt. Denn sind a, b, c die Wurzeln derselben Congruenz, so ist $a + b + c \equiv 0 \mathrm{M} p$, also $a + b + c$ entweder gleich p oder gleich 2p.

Hieraus folgt, dass a, b, c nicht gleichzeitig grösser als $\frac{2}{3}(p-1)$ sein und ausser dem Theiler 2 keinen grössten gemeinsamen Theiler besitzen können. Auch leuchtet ein, dass eine der Wurzeln einer der Formen $3n + 1$ oder $3n + 2$ angehören muss.

Abschnitt III.

I.

Ist $A = a^\alpha b^\beta c^\gamma$, wo a, b, c von einander verschiedene Primzahlen vorstellen, so soll die Anzahl der Dimensionen von a, b, c angegeben werden, welche die Binomialcoefficienten von A enthalten.

Hierzu führen folgende Wahrheiten:

1) Setzt man $A = ka^\alpha$, so sind die gebrochenen Factoren, mit denen man einen Binomialcoefficienten multiplicirt, um den folgenden zu erhalten, durch a unhebbar, falls der Zeiger dieses letztern durch a untheilbar ist.

Denn $(ka^\alpha)_{na} = (ka^\alpha)_{na-1} \cdot \frac{ka^\alpha - \overline{na-1}}{na}$.

Hieraus geht hervor, dass jeder Binomialcoefficient mit dem Zeiger na gegenüber seinem Vorgänger soviel Dimensionen von a verliert, als der Zeiger des erstern deren enthält.

2) Die gebrochenen Factoren, mit denen man einen Binomialcoefficienten multiplicirt, um den folgenden zu erhalten, sind durch a unhebbar, falls der Zeiger des letztern Binomialcoefficienten von der Form $na + 1$ ist.

Denn $(ka^\alpha)_{na+1} = (ka^\alpha)_{na} \cdot \frac{ka^\alpha - na}{na + 1}$.

Hieraus geht hervor, dass ein Binomialcoefficient mit dem Zeiger $na + 1$ gegenüber seinem Vorgänger soviel Dimensionen von a gewinnt, als die Anzahl der Dimensionen von a beträgt, welche na besitzt.

Aus 1) und 2) erhellt, dass die Binomialcoefficienten A_{na+1} und A_{na-1} die gleiche Anzahl von Dimensionen des Primfactors a besitzen.

3) Kein Binomialcoefficient, dessen Zeiger durch a untheilbar, kann gegenüber seinem Vorgänger einen Verlust an Dimensionen des Primfactors a erleiden.

Denn ist ν relative Primzahl gegen a, so ist $A_{na+\nu} = A_{na+\nu-1} \cdot \frac{ka^\alpha - \overline{na + \nu - 1}}{na + \nu}$.

4) Kein Binomialcoefficient, dessen Zeiger nicht von der Form $na + 1$ kann gegenüber seinem Vorgänger einen Gewinn an Dimensionen des Primfactors a erfahren.

Universitäts- und
Landesbibliothek Düsseldorf

Denn ist λ von 1 verschieden und kleiner als a — eine Annahme, die der Allgemeinheit keinen Eintrag thut — so ist

$A_{na+\lambda} = A_{na+\lambda-1} \cdot \frac{ka^{\alpha} - \overline{na + \lambda - 1}}{na + \lambda}$; hierin ist $ka^{\alpha} - \overline{na + \lambda - 1}$ durch a untheilbar.

Scheidet man nun von den Binomialcoefficienten der Zahl A die beiden A_0 und A_A aus, die beide der Einheit gleich sind, so erhellt, dass die übrigen in zwei Klassen gruppirt werden können. Diejenigen, deren Zeiger durch a untheilbar, sind sämmtlich durch a^{α} theilbar.

Diejenigen, deren Zeiger durch a theilbar, verlieren von den α Dimensionen des Primfactors so viele, als die Anzahl der Dimensionen von a beträgt, die der Zeiger enthält.

Auf diese Eigenschaften des Binomialcoefficienten lässt sich der direkte Beweis eines Satzes begründen, der in der Zahlentheorie von Bedeutung ist. Es ist nämlich

$$(\alpha + hp^{\mu})^t \equiv \alpha^t M p^{\mu+\nu},$$

worin α und h prim gegen p, während t durch p^{ν} theilbar. Denn entwickelt man $(\alpha + hp^{\mu})^t$ nach den binomischen Satz, so lassen sich die Glieder mit Ausnahme des ersten α^t in zwei Gruppen sondern, deren erste die Glieder enthält, in denen die Zeiger der Binomialcoefficienten von t durch p untheilbar, während in der zweiten Gruppe sämmtliche Glieder vorkommen, in denen die Zeiger der Binomialcoefficienten durch p theilbar sind.

Lässt man noch zur Vereinfachung die Potenzen von α und h, mit denen die Binomialcoefficienten multiplicirt erscheinen, fort, so ist ein Glied der erstern Gruppe von der Form $t_k p^{k\mu}$, worin k durch p untheilbar ist. Deshalb enthält t_k stets ν Dimensionen von p, mithin $t^k p^{k\mu}$ stets $\nu + k\mu$ Dimensionen von p.

Die Glieder der zweiten Gruppe ordne man, wie folgt:

$$\begin{array}{ll} t_p p^{p\mu}, & t_{2p} p^{2p\mu} \quad \ldots\ldots\ldots\ldots \\ t_{p^2} p^{p^2\mu}, & t_{2p^2} p^{2p^2\mu}, \quad \ldots\ldots\ldots\ldots \quad \text{A)} \\ \vdots & \vdots \\ t_{p^\nu} \cdot p^{p^\nu\mu}, & t_{2p^\nu} \cdot p^{2p^\nu\mu} \quad \ldots\ldots\ldots \end{array}$$

Die Binomialcoefficienten, welche derselben Horizontalreihe angehören, wie

$$\begin{array}{ll} t_p, & t_{2p}, \\ t_{p^2}, & t_{2p^2}, \\ \vdots & \vdots \\ t_{p^\nu}, & t_{2p^\nu}, \end{array}$$

haben dieselbe Anzahl vön Dimensionen von p.

Ferner hat jedes Anfangsglied einer Horizontalreihe unter sämmtlichen Gliedern derselben Reihe, die kleinste Anzahl ven Dimensionen von p.

Um also sicher zu sein, dass die Glieder der Reihe A durch $p^{\mu+\nu}$ theilbar sind, hat man diese Wahrheit nur von den Anfangsgliedern zu erweisen, d. h. es müssen folgende Relationen gelten:

$$\begin{array}{ll} p\mu + \nu - 1 & \geqq \mu + \nu, \\ p^2\mu + \nu - 2 & \geqq \mu + \nu, \\ \vdots & \vdots \quad \vdots \\ p^\nu\mu & \geqq \mu + \nu. \end{array}$$

Universitäts- und
Landesbibliothek Düsseldorf

Diesen Relationen genügt $p = 2$; denn ist λ irgend eine der Zahlen $1, 2, 3, \ldots \nu$, so ist $2^\lambda \mu + \nu - \lambda \geqq \mu + \nu$, oder $2^\lambda \mu + \lambda \geqq \mu$, d. h. $\mu \geqq \frac{\lambda}{2^\lambda - 1}$, eine Beziehung, der jeder Werth von μ der positiv und von Null verschieden ist, Genüge leistet.

Aus Vorstehendem folgt: Der Gruppe der Relationen B) genügt $p = 2$, um so mehr jede grössere Primzahl für p; ν darf irgend eine ganze Zahl mit Einschluss von Null sein, während μ von Null verschieden sein muss.

Zweitens ist $(\alpha + hp^\mu)^t \equiv \alpha^t + t\alpha^{t-1} hp^\mu \, Mp^{\mu+\nu+1}$ C).

Denn entwickelt man $(\alpha + hp^\mu)^t$ und vertheilt sämmtliche Glieder mit Ausnahme von α^t und $t\alpha^{t-1}hp^\mu$, ähnlich wie vorhin, in zwei Gruppen, so enthält jedes Glied der Form $t_k p^{k\mu}$ $k\mu + \nu$ Dimensionen von p, ist also durch $p^{k\mu+\nu}$, daher auch durch $p^{\mu+\nu+1}$ theilbar, weil $k\mu + \nu$ stets $\geqq \mu + \nu + 1$ ist, falls μ positiv und von Null verschieden.

Sollen die Glieder der zweiten Gruppe einzeln durch $p^{\mu+\nu+1}$ theilbar sein, so müssen folgende Relationen bestehen:

$$\begin{array}{ll} p\mu + \nu - 1 & \geqq \mu + \nu + 1 \\ p^2\mu + \nu - 2 & \geqq \mu + \nu + 1 \quad \text{D)}. \\ \vdots & \quad \vdots \quad \vdots \\ p^\nu \mu & \geqq \mu + \nu + 1 \end{array}$$

Hierbei ist zu unterscheiden, ob $p = 2$ oder eine ungerade Primzahl ist.

Ist $p = 2$, so muss $\mu > 1$ sein, wenn anders die Relation $p\mu + \nu - 1 \geqq \mu + \nu + 1$ bestehen soll; ist aber $\mu > 1$, so bestehen die Relationen D) zu Recht. Denn ist λ eine der Zahlen von 1 bis ν, so ist $2^\lambda \mu + \nu - \lambda \geqq \mu + \nu + 1$; hieraus $\mu \geqq \frac{\lambda + 1}{2^\lambda - 1}$, ferner ist 2 der grösste Werth von $\frac{\lambda + 1}{2^\lambda - 1}$.

Ist p eine ungerade Primzahl und μ mindestens der Einheit gleich, so bestehen die Relationen D) um so mehr.

Aus Vorstehendem folgt, dass die Congruenz C) stets besteht, falls p eine ungerade Primzahl ist und gleichzeitig $\mu \geqq 1$; ist aber $p = 2$, so muss $\mu > 1$ sein.

2.

Das Quadrat der Facultät von $\frac{p-1}{2}$ ist der negativen Einheit congruent, wenn p eine ungerade Primzahl ist. Denn

$$\begin{array}{ccc} 1 & \equiv & 1 \, Mp, \\ 2 & \equiv & 2 \\ \vdots & & \vdots \\ \frac{p-1}{2} & \equiv & \frac{p-1}{2} \\ \frac{p+1}{2} & \equiv & -\frac{p-1}{2} \\ \frac{p+3}{2} & \equiv & -\frac{p+3}{2} \\ \vdots & & \vdots \\ p-1 & \equiv & -1 \\ \hline (p-1)! & \equiv & -1 \equiv \left(\frac{p-1}{2}!\right)^2 Mp. \end{array}$$

Universitäts- und
Landesbibliothek Düsseldorf

3.

Die Zerlegung von Congruenzen in reelle lineare Factoren, falls der Modul die Potenz einer Primzahl ist.

Bisher weiss man allgemein nur diejenigen Congruenzen in lineare reelle Factoren zu zerlegen, in denen der Modul prim ist, während gleichzeitig die Anzahl der Wurzeln mit dem Grade der Congruenz übereinstimmt. Um so interessanter ist es, diejenigen Fälle zu sammeln, in denen die Zerlegung nur von einer der erwähnten Bedingungen abhängt. Im Folgenden soll nun nachgewiesen werden, dass 1) $x^t - 1 \equiv 0 \mathrm{M} p^n$, falls t Theiler von $p - 1$ ist, stets in reelle lineare Formen zerlegt werden kann.

Bekanntlich hat diese Congruenz zufolge der für t gestellten Bedingung stets t Wurzeln, ebenso wie die Congruenz 2) $x^t - 1 \equiv 0 \mathrm{M} p$.

Seien $\alpha, \beta, \gamma, \ldots \mu$ die Wurzeln der letztern, die t an Zahl sämmtlich zwischen 1 und $p - 1$ liegen, d. h. für den Modul p sämmtlich incongruent sind, so sind die Wurzeln von 1) $\alpha + k_1 p, \beta + k_2 p, \ldots \mu + k_t p$, wofür wir zur Abkürzung $\alpha_1, \beta_1, \ldots \mu_1$ setzen.

Nun ist ersichtlich, dass α_1, β_1, μ_1 ebenfalls nach dem Modul p incongruent sind. Ferner ist $x^t - 1 \equiv (x - \alpha_1)\varphi_1 x \mathrm{M} p^n$, wo $\varphi_1 x$ vom Grade $t - 1$, während der Coefficient der höchsten Potenz von x der Einheit gleicht, daher muss $\varphi_1 x \equiv 0 \mathrm{M} p^n$ die Wurzeln β_1, γ_1, μ_1 besitzen. Andernfalls müsste der Congruenz $x - \alpha_1 \equiv 0 \mathrm{M} p^n$ eine der Grössen β_1, γ_1, μ_1, genügen, was nach dem Vorigen unmöglich ist. Ebenso hat man $\varphi_1 x \equiv (x - \beta_1)\varphi_2 x \mathrm{M} p^n$, worin φ_2 vom Grade $t - 2$, während der Coefficient der höchsten Potenz der Unbekannten der Einheit gleicht. Darum muss $\varphi_2 x \equiv 0 \mathrm{M} p^n$ die Wurzeln $\gamma_1, \ldots \mu_1$ besitzen, weil andernfalls $x - \beta_1 \equiv 0 \mathrm{M} p^n$ durch eine der Grössen $\gamma_1, \ldots \mu_1$ befriedigt werden müsste.

Hieraus folgt, dass die Congruenz $(x^t - 1) \equiv (x - \alpha_1)(x - \beta_6) \ldots (x - \mu_1) \mathrm{M} p^n$ identisch ist.

Beispiel: Sei zu lösen 1) $x^4 \equiv 1 \mathrm{M} 25$; die 4 Wurzeln von 2) $x^4 \equiv 1 \mathrm{M} 5$ sind 1, 2, 3, 4. Bezeichnet man mit a eine dieser Zahlen, so sind die Wurzeln von 1) von der Form $a + 5h$. Der Werth von h bestimmt sich durch $(a + 5h)^4 \equiv 1 \mathrm{M} 25$, hieraus 3) $\frac{a^4 - 1}{5} + a^3 h \equiv 0 \mathrm{M} 5$.

Combinirt man die 4 Werthe von a mit den 4 Werthen von h aus 3), so ergeben sich 1, 7, 18, 24 als Wurzeln von 1).

Hiernach ist $x^4 - 1 \equiv (x - 1)(x - 7)(x - 18)(x - 24) \mathrm{M} 25$.

Ist $x^3 \equiv 1 \mathrm{M} 49$ zu lösen, so sind die Werthe von $\sqrt[3]{1} \mathrm{M} 7$ gleich 1, 2, 4. Deshalb sind die Werthe von $\sqrt[3]{1} \mathrm{M} 49$ von den Formen $1 + 7h$, $2 + 7h$, $4 + 7h$. Bezeichnet man mit a eine der Zahlen 1, 2, 4, so ergeben sich die Werthe von h aus der Congruenz: $\frac{a^3 - 1}{7} + 3a^2 h \equiv 0 \mathrm{M} 7$.

Hiernach sind die 3 Werthe von $\sqrt[3]{1} \mathrm{M} 49$ die folgenden: 1, 30, 18, und man hat identisch: $x^3 - 1 \equiv (x - 1)(x - 30)(x - 18) \mathrm{M} 49$, woraus folgt

$$1 + 30 + 18 \equiv 0 \mathrm{M} 49,$$
$$30 + 18 + 540 \equiv 0,$$
$$1 \,.\, 30 \,.\, 18 \equiv 1.$$

Universitäts- und
Landesbibliothek Düsseldorf

Es ist leicht ersichtlich, wie sehr dieser Satz die Lösung dieser Art von Congruenzen unter Umständen erleichtert, da man für jede gefundene Wurzel den Grad der Congruenz durch Division mit dem Wurzelfactor um eine Einheit erniedrigen kann.

4.

Ueber eine Klasse von quadratischen Congruenzen, deren Wurzeln niemals reell sind.

Ist p eine Primzahl der Form $6n + 5$ und r kleiner als p, so hat die Congruenz $x^3 \equiv r M p$ bekanntlich nur eine einzige reelle Wurzel, die α heissen möge.

Nun ist $x^3 - r = (x - \alpha)(x^2 + \alpha x + \alpha^2) + \alpha^3 - r$. Hieraus folgt, dass das Product $(x - \alpha)(x^2 + \alpha x + \alpha^2)$ nur für diejenigen reellen Werthe von x durch p theilbar wird, für welche $x^3 - r$ durch p theilbar ist, d. h. die Wurzeln von $x^2 + \alpha x + \alpha^2 \equiv 0 M p$ können nicht reell sein, während α eine beliebige Zahl zwischen 1 und $p - 1$ vorstellt. So haben die Congruenzen

$$x^2 + x + 1 \equiv 0 M 5,$$
$$x^2 + 2x + 4 \equiv 0,$$
$$x^2 + 3x + 9 \equiv 0,$$
$$x^2 + 4x + 16 \equiv 0$$

keine reellen Wurzeln.

Diese Wahrheit lässt sich leicht verallgemeinen.

Sind a, b, c Primzahlen der Form $6n + 5$ in beliebiger Anzahl und α kleiner als die kleinste derselben, so können die Wurzeln von $x^2 + \alpha x + \alpha^2 \equiv 0 M (a . b . c \ldots)$ nicht reell sein.

5.

Reste der Potenzen vom fünften Grade.

Durch Specialisirung der in Abschnitt I. gefundenen Sätze lassen sich leicht folgende Behauptungen erweisen.

Ist p eine Primzahl, aber nicht von der Form $5n + 1$, so sind alle Zahlen von 1 bis $p - 1$ Reste der Potenzen vom fünften Grade oder kürzer Reste vom fünften Grade. Deshalb ist die Congruenz $x^5 \equiv r M p$, worin r prim gegen p, stets lösbar, und besitzt eine einzige reelle Wurzel, falls die Primzahl p einer der Formen $10n + 3$, $10n + 7$, $10n + 9$ angehört. Dagegen hat 1) $x^4 + \alpha x^3 + \alpha^2 x^2 + \alpha^3 x + \alpha^4 \equiv 0 M p$ niemals reelle Wurzeln, wenn α gegen p prim ist.

Sind ferner $p_1, p_2, \ldots$ Primzahlen, die sämmtlich der Form $10n + 1$ nicht angehören, so besitzt $x^5 \equiv r M (p_1, p_2, \ldots)$ stets eine und nur eine reelle Wurzel, während die Congruenz 1) nach dem Product der Moduln $p_1, p_2 \ldots$ niemals reelle Wurzeln hat. Ist zweitens p von der Form $5n + 1$, so ist die Anzahl der Reste vom fünften Grade $\frac{1}{5}(p - 1)$, die der Nichtreste $\frac{4}{5}(p - 1)$. Denn ist a Primitivwurzel für p, so sind die Reste der Potenzen $a^5, a^{2 \cdot 5}, a^{3 \cdot 5}, \ldots a^{\frac{p-1}{5} \cdot 5}$ sämmtlich von einander verschieden und stellen die Reste vom fünften Grade für den Modul p vor. Alle andern Zahlen in der Reihe von 1 bis $p - 1$ sind Nichtreste; denn ihre Indices sind durch fünf untheilbar.

Universitäts- und
Landesbibliothek Düsseldorf

Soll eine Zahl Rest sein, so muss sie der Bedingung $x^{2m} \equiv 1 \mathrm{Mp}^n$ genügen, wenn man $p = 10m + 1$ setzt. Diese Congruenz enthält sämmtliche Reste als Wurzeln, auch lehrt ihre Form, dass das Product zweier Reste wiederum ein Rest ist, sowie dass $+r$ und $-r$ gleichzeitig Reste sind.

Soll eine Zahl Nichtrest sein, so muss sie der Bedingung $x^{8m} + x^{6m} + x^{4m} + x + {}^{2m} 1 \equiv 0$ genügen, auch leuchtet ein, dass $+n$ und $-n$ gleichzeitig Nichtreste sind, da die Exponenten der Potenzen von x sämmtlich gerade sind.

Ferner hat der Ausdruck $\sqrt[3]{r}\mathrm{Mp}$ fünf reelle Wurzeln oder keiue, je nachdem r Rest oder Nichtrest ist. Sind im erstern Falle a, b, c, d, e die fünf Werthe des Ausdrucks $\sqrt[5]{r}\mathrm{Mp}$, so ist stets $a + b + c + d + e \equiv 0 \mathrm{Mp}$. Da nun die Summe der Wurzeln das Product $5(p-1)$ zur obern Grenze hat, welche sie nicht erreichen kann, so muss mindestens eine der Wurzeln unterhalb $\frac{4}{5}(p-1)$ liegen.

Hieraus folgt, dass ein Rest vom fünften Grade einer Primzahl der Form $10m + 1$ jedenfalls der fünften Potenz einer Zahl congruent ist, die $\frac{4}{5}(p-1)$ nicht übersteigt.

Auch können die Wurzeln nicht gleichzeitig durch 5 theilbar sein. Denn wäre $a = 5\alpha$, $b = 5\beta$, $c = 5\gamma$, $d = 5\delta$, $e = 5\varepsilon$, so könnte höchstens eine der Grössen $\alpha, \beta, \gamma, \delta, \varepsilon$ gleich $\frac{p-1}{5}$, alle andern müssten kleiner als $\frac{p-1}{5}$ sein. Es ist aber

$$5(\alpha + \beta + \gamma + \delta + \varepsilon) \equiv 0 \mathrm{Mp} \text{ oder } \alpha + \beta + \gamma + \delta + \varepsilon \equiv 0 \mathrm{Mp},$$

was unmöglich ist, da die Summe von $\alpha, \beta, \gamma, \delta, \varepsilon$ den Werth $p - 1$ keinesfalls erreicht.

Das vorige Resultat lässt sich auch folgenderweise ausdrücken: Ist r Rest vom fünften Grade für die Primzahl p, welche von der Form $5n + 1$ ist, so muss einer der fünf Werthe von $\sqrt[5]{r}\mathrm{Mp}$ einer der Formen $5k + 1$, $5k + 2$, $5k + 3$ oder $5k + 4$ angehören und der gemeinsame Theiler der fünf Werthe kann nur 2, 3 oder 4 sein.

6.

Die Beziehung der Einheitswurzeln zu den Resten und Nichtresten und eine darauf beruhenden Eintheilung der Nichtreste.

Sei p von der Form $6n + 1$, so muss ein kubischer Rest für p der Congruenz $x^{\frac{p-1}{3}} \equiv 1 \mathrm{Mp}$ genügen. Die Nichtreste zur $\frac{p-1}{3}$ten Potenz erhoben, lassen nur zwei verschiedene Reste; nennt man dieselben ε und ε_1, so sind 1, ε und ε_1 die 3 Einheitswurzeln für den Modul p, d. h. die 3 Werthe von $\sqrt[3]{1}\mathrm{Mp}$. Denn ist a kubischer Nichtrest, so ist $a^{\frac{p-1}{3}} \equiv \varepsilon$, wo ε von der Einheit verschieden und ε^3 muss, wie leicht ersichtlich, der positiven Einheit congruent sein. Ist ferner ε eine von der positiven Einheit verschiedene Einheitswurzel, so sind die drei Werthe von $\sqrt[3]{1}\mathrm{Mp}$ $\varepsilon, \varepsilon^2, \varepsilon^3$; dieselben sind incongruent.

Ist α durch p untheilbar und bezeichnet man den kleinsten positiven Rest von $\alpha^{\frac{p-1}{3}}$ für den Modul p, nach Analogie der quadratischen Reste mit $\left(\frac{\alpha}{p}\right)$, so ist α kubischer Rest oder Nichtrest, je nachdem $\left(\frac{\alpha}{p}\right) = 1$ oder gleich ε oder ε^2 ist.

Hiernach lassen sich die Nichtreste in zwei Klassen theilen. Für die der erstern hat man stets $\left(\frac{\alpha}{p}\right) = \varepsilon$, für die der andern $\left(\frac{\beta}{p}\right) = \varepsilon^2$.

Universitäts- und
Landesbibliothek Düsseldorf

Zwei Nichtreste derselben Klasse geben einen Nichtrest, zwei Nichtreste verschiedener Klassen einen Rest zum Product. Denn sind α und α_1 etwa zwei Nichtreste der erstern Klasse, so ist $\alpha^{\frac{p-1}{3}} \equiv \varepsilon$,

$$\alpha_1^{\frac{p-1}{3}} \equiv \varepsilon, \text{ also } (\alpha\alpha_1)^{\frac{p-1}{3}} \equiv \varepsilon^2.$$

Sind α und α_1 zwei Nichsreste der zweiten Klasse, so ist $(\alpha\alpha_1)^{\frac{p-1}{3}} \equiv \varepsilon$. Daraus ersieht man ferner, dass das Product zweier Nichtreste der einen Klasse — der andern Elasse angehört.

Dagegen ist das Product zweier Nichtreste verschiedener Klassen stets kubischer Rest. Denn ist $\alpha^{\frac{p-1}{3}} \equiv \varepsilon$,

$$\beta^{\frac{p-1}{3}} \equiv \varepsilon^2,$$

$$(\alpha\beta)^{\frac{p-1}{3}} \equiv 1.$$

Auch leuchtet ein, dass ε^t mit ε, ε^2, ε^3 congrnent ist, je nachdem

$$t \equiv 1 \text{ M}3,$$
$$t \equiv 2,$$
$$t \equiv 0 \text{ ist.}$$

Beispiel: Kubische Reste für 7 sind 1, 6, Nichtreste: 2, 3, 4, 5. Soll eine Zahl Rest sein, so muss sie der Congruenz $x^2 \equiv 1$ M7 genügen. Die 3 Werthe von $\sqrt[3]{1}$ Mp sind 1, 2, 4. Es sind also die Quadrate der zwei kubischen Reste 1 und $6 \equiv 1$, und die Quadrate der 4 kubischen Nichtreste: 2, 3, 4, 5 entweder $\equiv 2$ oder $\equiv 4$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$ M7.

Kubische Reste für 13 sind 1, 5, 8, 12, Nichtreste 2, 3, 4, 6, 7, 9, 10, 11. Die Reste genügen der Congruenz $x^4 \equiv 1$ M13.

Die 3 Werthe von $\sqrt[3]{1}$ M13 sind 1, 3, 9, also müssten die Biquadrate der Nichtreste einer der Zahlen 3 oder 9 congruent sein; nun ist $2^4 \equiv 3^4 \equiv 10^4 \equiv 11^4 \equiv 3$ M13 und $4^4 \equiv 6^4 \equiv 7^4 \equiv 9^4 \equiv 9$ M13.

Tafel der kubischen Reste aller Primzahlen von der Form 6n + 1 von 1 bis 97 nebst den Resten der Zahlen 3, 9, 27, 81.

3	1	2																														
7	1	6																														
9	1	8																														
13	1	5	8	12																												
19	1	7	8	11	12	18																										
27	1	8	10	17	19	26																										
31	1	2	4	8	15	16	23	27	29	30																						
37	1	6	8	10	11	14	23	26	27	29	31	36																				
43	1	2	4	8	11	16	21	22	27	32	35	39	41	42																		
61	1	3	8	9	11	20	23	24	27	28	33	34	37	38	41	50	52	53	58	60												
67	1	3	5	8	9	14	15	22	24	25	27	40	42	43	45	52	53	58	59	62	64	66										
73	1	3	7	8	9	10	17	21	22	24	27	30	43	46	49	51	52	56	63	64	65	66	70	72								
79	1	8	10	12	14	15	17	18	21	22	27	33	38	41	46	52	57	58	61	62	64	65	67	69	71	78						
81	1	8	10	17	19	26	28	35	37	44	46	53	55	62	64	71	73	80														
97	1	8	12	18	19	20	22	27	28	30	33	34	42	45	46	47	50	51	52	55	63	64	67	69	70	75	77	78	79	85	89	96

Universitäts- und
Landesbibliothek Düsseldorf