Ueber Congruenzgruppen von Primzahlstufe.

Von

JOSEPH GIERSTER in Bamberg.

Anschliessend an meine früheren Arbeiten über elliptische Modulfunctionen, wie dieselben in den Bänden 17, 18, 21 dieser Annalen veröffentlicht sind, werden in der vorliegenden kurzen Arbeit sämtliche Congruenzgruppen von Primzahlstufe (§ 1, § 2) aufgestellt. Nachdem in § 3 eine allgemeine Methode zur Bestimmung des Geschlechtes dieser Gruppen nach der Klein'schen Definition erläutert ist, wird in § 4 eine Tabelle des Geschlechtes für die genannten Gruppen hingeschrieben. Aus dieser Tabelle werden dann in § 5 leicht die sämtlichen Hauptmoduln von Primzahlstufe d. h. diejenigen Moduln abgelesen, welche einer Congruenzgruppe vom Geschlechte Null entsprechen.

Es ergeben sich ausser den Moduln der dritten und fünften Stufe nur noch Hauptmoduln der siebenten, elften und dreizehnten Stufe.

§ 1.

Allgemeines über Congruenzgruppen der q^{ten} Stufe.

Im 18^{ten} Bande dieser Annalen, pag. 319ff. habe ich alle Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades bestimmt. Ich werde nunmehr zeigen, dass hiermit eo ipso alle Congruenzgruppen von Primzahlstufe gefunden sind.

Eine „Congruenzgruppe“) der q^{ten} Stufe“ ist dadurch definirt, dass sie aus *allen* ganzzahligen Substitutionen

$$(1) \quad \omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$$

der Determinante $\alpha\delta - \beta\gamma = 1$ besteht, deren $\alpha, \beta, \gamma, \delta$ bestimmte

*) F. Klein, Sitzungsab. der Münchener Akademie, Sitz. v. 6. Dez. 1879 oder Math. Ann. Bd. XVII, pag. 63ff. Blosser Citate auf Seitenzahlen beziehen sich auf diese Arbeit. Hurwitz, Mathem. Ann. Bd. XVIII, pag. 540ff.

Bedingungen modulo q erfüllen und zwar muss q die kleinste ganze Zahl sein, für welche dies der Fall ist. Die genannten Bedingungen werden nur für eine endliche Anzahl r von Lösungen $\alpha_v, \beta_v, \gamma_v, \delta_v$ modulo q erfüllt sein, da die Congruenz $\alpha\delta - \beta\gamma \equiv 1 \pmod{q}$, welche immer stattfinden muss, selbst nur die endliche Zahl von $\frac{q(q^2-1)}{2}$ Lösungen hat. Diese r Lösungen liefern (modulo q) r Substitutionen

$$(2) \quad S_v \equiv \frac{\alpha_v \omega + \beta_v}{\gamma_v \omega + \delta_v} \pmod{q}.$$

Alle ganzzahligen linearen Substitutionen der Determinante 1, welche mod. q zu einer S_v congruent sind, gehören nach Definition der Congruenzgruppe an.

Ich will die Substitutionen der letzteren mit σ_v bezeichnen.

Aus dem Begriffe der Gruppe folgt sogleich, dass, wenn σ_1 und σ_2 zwei Substitutionen der Congruenzgruppe sind, auch $\sigma_1 \cdot \sigma_2$ eine solche sein muss. Also müssen auch die r Substitutionen S_v (2) eine Gruppe G_r bilden und diese Gruppe ist offenbar eine in der Galois'-Gruppe G der Modulargleichungen für q enthaltene Untergruppe.

Die Gruppe G besteht nämlich aus den $\frac{q(q^2-1)}{2}$ Substitutionen S_v zu welchen alle ganzzahligen linearen Substitutionen (1) der Determinante 1 modulo q congruent sind*).

Weiterhin folgt, dass unter den Substitutionen S_v immer auch die Identität $\omega' \equiv \omega \pmod{q}$ enthalten ist, und dass also jede Congruenzgruppe der q^{ten} Stufe die ausgezeichnete, durch die Bedingungen $\alpha\delta - \beta\gamma \equiv 1, \alpha : \beta : \gamma : \delta \equiv 1 : 0 : 0 : 1 \pmod{q}$ definierte Congruenzgruppe der q^{ten} Stufe als Untergruppe enthält.

Wir können jetzt folgenden Satz aussprechen:

Man erhält alle Congruenzgruppen der q^{ten} Stufe, wenn man der Reihe nach alle Untergruppen G_r der Galois'schen Gruppe G der Modulargleichungen für q (mit Ausschluss von G selbst) betrachtet und jedesmal alle jene Substitutionen (1) nimmt, welche zu einer Substitution S_v der betrachteten Untergruppe modulo q congruent sind.

Jedenfalls bilden nämlich diese Substitutionen eine Gruppe g , für welche die $\alpha, \beta, \gamma, \delta$ gegebenen Bedingungen modulo q (nämlich einer der r Bedingungen $\alpha : \beta : \gamma : \delta \equiv \alpha_v : \beta_v : \gamma_v : \delta_v \pmod{q}$) genügen. Dass aber q die Stufe der Congruenzgruppe ist, dass also die Zahl q bei Definition der betreffenden Substitutionen durch keine kleinere Zahl ersetzt werden kann, ist sehr einfach zu zeigen. Wäre nämlich die Stufe $q' < q$, so enthielte die Gruppe die ausgezeichnete Congruenzgruppe der q' -Stufe, also jedenfalls auch die beiden Substitutionen

*) Vergl. meinen schon citirten Aufsatz im 18^{ten} Bande der Mathem. Annalen.

$$\omega' = \omega + r q', \quad \omega' = \frac{(m q' + 1) \omega + n q'}{s q' \omega + (t q' + 1)},$$

wobei $(m q' + 1)(t q' + 1) - s n q'^2 = 1$ ist. Da aber q' zu q relativ prim wäre, so könnte man die Grössen r, m, n, s, t so bestimmen, dass die letztgenannten Substitutionen modulo q zu

$$\omega' \equiv \omega + 1 \quad \text{und} \quad \omega' \equiv -\frac{1}{\omega}$$

congruent wären. Dann würde aber bekanntlich die Gruppe G_r mit G selbst zusammenfallen, ein Fall der ausgeschlossen ist.

Man kann die Beziehung, welche hiernach zwischen den Untergruppen von G und den Congruenzgruppen besteht, als einen *Isomorphismus* bezeichnen, nur dass die Stufe dieses Isomorphismus eine unendlich hohe ist, indem jeder Substitution von G jedesmal unendlich viele Substitutionen der Congruenzgruppe entsprechen.

§ 2.

Aufzählung aller Congruenzgruppen der q^{ten} Stufe.

Nach § 1 ist klar, dass jeder Untergruppe G_r der Galois'schen Gruppe G der Modulargleichungen für q eine Congruenzgruppe der q^{ten} Stufe entspricht und umgekehrt. Man erkennt ferner sogleich, dass gleichberechtigten Untergruppen G_r auch gleichberechtigte Congruenzgruppen entsprechen und umgekehrt.

Bezeichnet ferner r die Ordnung der Untergruppe G_r , so hat die zugehörige Congruenzgruppe g_n den Index*)

$$n = \frac{q(q^2 - 1)}{2r},$$

d. h. ihre Substitutionen bilden den n^{ten} Theil aller ganzzahligen Substitutionen (1) der Determinante 1.

Dieses vorausgesetzt, erhält man unter Bezugnahme auf meine Arbeit in Band XVIII folgende

Tabelle der Congruenzgruppen der q^{ten} Stufe.

Congruenzgruppen.	Entsprechende Untergruppen von G .
I. <i>Es giebt:</i>	
<i>Eine $g_{\frac{q(q^2-1)}{2}}$</i>	<i>Eine $G_{(1)}$ -</i>
(die ausgezeichnete Congruenzgruppe der q^{ten} Stufe)	(die Identität).

*) pag. 63.

Congruenzgruppen.

Entsprechende Untergruppen von G .II. *Es gibt:*

a) $(q+1) \quad \frac{\mathfrak{S}_{q^2-1}}{2}$

b) $\frac{q(q+1)}{2} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{2\sigma}$

c) $\frac{q(q-1)}{2} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{2\tau}$

$$\left. \begin{array}{ll} (q+1) & G_q \\ \frac{q(q+1)}{2} & G_\sigma \\ \frac{q(q-1)}{2} & G_\tau \end{array} \right\} \text{(Cyklen).}$$

III. *Es gibt:*

$(q+1) \quad \frac{\mathfrak{S}_{q^2-1}}{2\sigma}$

$(q+1) \quad G'_{q,\sigma}$
(Die halbmetacyklischen Gruppen und ihre Untergruppen).

IV. *Es gibt:*

a) $\frac{q(q^2-1)}{4\sigma'} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{4\sigma'} \text{ oder}$

$\frac{q(q^2-1)}{4\sigma'} \quad G'_{2\sigma'} \text{ oder}$

2 A. v. je $\frac{q(q^2-1)}{8\sigma'} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{4\sigma'},$

2 A. v. je $\frac{q(q^2-1)}{8\sigma'} \quad G'_{2\sigma'},$

je nachdem $\frac{q-1}{2\sigma'}$ ungerade oder gerade ist;

b) $\frac{q(q^2-1)}{4\tau'} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{4\tau'} \text{ oder}$

$\frac{q(q^2-1)}{4\tau'} \quad G'_{2\tau'} \text{ oder}$

2 A. v. je $\frac{q(q^2-1)}{8\tau'} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{4\tau'},$

2 A. v. je $\frac{q(q^2-1)}{8\tau'} \quad G'_{2\tau'},$

je nachdem $\frac{q+1}{2\tau'}$ ungerade oder gerade ist;

c) $\frac{q(q^2-1)}{24} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{8} \text{ oder}$

$\frac{q(q^2-1)}{24} \quad G'_4 \text{ oder}$

2 A. v. je $\frac{q(q^2-1)}{48} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{8},$

2 A. v. je $\frac{q(q^2-1)}{48} \quad G'_4,$

je nachdem $\binom{2}{q} = -1$ oder $= +1$ ist.V. *Es gibt:*

$\frac{q(q^2-1)}{24} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{24} \text{ oder}$

$\frac{q(q^2-1)}{24} \quad G''_{12} \text{ oder}$

2 A. v. je $\frac{q(q^2-1)}{48} \quad \frac{\mathfrak{S}_{q(q^2-1)}}{24},$

2 A. v. je $\frac{q(q^2-1)}{48} \quad G''_{12},$

(Tetraedergruppen)

je nachdem $\binom{2}{q} = -1$ oder $= +1$ ist.

(Doppelpyramidengruppen)

(Die in I, II, III, IV, V aufgezählten Gruppen existiren für jede Primzahl $q > 3$).

VI. Es giebt:

$$2 \text{ A. v. je } \frac{q(q^2-1)}{48} \quad \mathfrak{G}_{\frac{q(q^2-1)}{48}} \quad \left| \quad 2 \text{ A. v. je } \frac{q(q^2-1)}{48} \quad G''_{24}, \quad (\text{Oktaedergruppen}), \right.$$

nur wenn $\binom{2}{q} = +1$ ist.

VII. Es giebt:

$$2 \text{ A. v. je } \frac{q(q^2-1)}{120} \quad \mathfrak{G}_{\frac{q(q^2-1)}{120}} \quad \left| \quad 2 \text{ A. v. je } \frac{q(q^2-1)}{120} \quad G''_{60} \quad (\text{Ikosaedergruppen}), \right.$$

nur wenn $q \equiv \pm 1 \pmod{5}$ ist.

In dieser Tabelle bedeutet σ einen von 1 verschiedenen Theiler von $\frac{q-1}{2}$ (incl. $\frac{q-1}{2}$), τ einen von 1 verschiedenen Theiler von $\frac{q+1}{2}$ (incl. $\frac{q+1}{2}$); σ' und τ' bedeuten dieselben Zahlen wie σ und τ mit Ausschluss des Theilers 2. Ferner ist z. B. Nr. V in folgender Weise zu lesen: Es giebt entweder $\frac{q(q^2-1)}{24}$ gleichberechtigte Congruenzgruppen g vom Index $\frac{q(q^2-1)}{24}$, deren entsprechende Untergruppen G''_{12} Tetraedergruppen sind, oder 2 Arten von je $\frac{q(q^2-1)}{48}$ gleichberechtigten solchen Gruppen, je nachdem 2 quadratischer Nichtrest oder Rest mod. q ist.

Den aufgestellten Congruenzgruppen der q^{ten} Stufe entsprechen ebensoviele volle Congruenzmodulsysteme der q^{ten} Stufe*). Es sollen volle Modulsysteme, welche gleichberechtigten Congruenzgruppen g entsprechen, ebenfalls gleichberechtigt genannt werden. Ich stelle hier einige Sätze über die Modulsysteme zusammen, welche später verwendet werden, übrigens aber aus der allgemeinen Theorie hervorgehen**).

1) Ist die Untergruppe G_r , welche zur Congruenzgruppe g_n gehört, eine Untergruppe der Gruppe G_r' , welche zur Congruenzgruppe g_n' gehört, so lassen sich die Moduln, welche zur letzteren Gruppe gehören, rational durch die Moduln des zur ersteren Gruppe gehörigen vollen Modulsystems darstellen. Insbesondere lassen sich alle Moduln als rationale Functionen der ausgezeichneten Moduln derselben Stufe darstellen und die rationale absolute Invariante J ist eine rationale Function der Moduln jedes vollen Modulsystems***).

*) pag. 64.

**) pag. 66 ff.

***) Wegen der Bezeichnungen vergleiche durchweg die bereits citirten Arbeiten.

2) Denkt man sich die Moduln eines Modulsystems der q^{ten} Stufe als rationale Functionen der ausgezeichneten Moduln der q^{ten} Stufe dargestellt, so erhält man *alle* zu dem einen System gleichberechtigten Modulsysteme, wenn man in den genannten rationalen Functionen die ausgezeichneten Moduln den Substitutionen der Gruppe $\Gamma^*)$ unterwirft. Daraus folgt dann leicht, dass alle zu einem Modul gleichberechtigten Moduln die Wurzeln einer *irreductiblen* algebraischen Gleichung sind, deren Coefficienten rationale Functionen von J sind.

§ 3.

Berechnung des Geschlechtes der Congruenzgruppen der q^{ten} Stufe.

Zu jeder Congruenzgruppe vom Index n gehört ein Fundamentalpolygon**), welches aus $2n$ Elementardreiecken besteht und dessen Randpunkte und Kanten paarweise als relativ äquivalent zusammengehören. Schneidet man dieses Polygon aus der Ebene heraus und heftet die Paare zusammengehöriger Kanten zusammen, so erhält man eine geschlossene Fläche, deren Geschlecht (im Sinne der geometria situs aufgefasst) nach F. Klein *das Geschlecht p der Congruenzgruppe g* heisst.

Diese Zahl p lässt sich durch die Bemerkung finden, dass sich auf der erwähnten geschlossenen Fläche ein vollständiges Netz von $2n$ Elementardreiecken construiren lässt***). Bezeichnet man bez. mit E, F, K die Zahlen der Ecken, Flächen und Kanten dieses Netzes, so ergibt der erweiterte Euler'sche Polyedersatz das Geschlecht p durch die Gleichung:

$$(1) \quad 2(p-1) = K - F - E.$$

Leicht lässt sich diese Gleichung in eine andere Gestalt bringen. Man bemerke zu diesem Zwecke, dass $F = 2n$ und $K = 3n$ ist, dass sich

ferner $E = 3n - \sum_{v=1}^{v=E} (e_v - 1)$ ergibt, wenn man mit $2e_1, 2e_2, \dots, 2e_v, \dots$ die Zahlen der Elementardreiecke bezeichnet, welche bez. in der $1^{\text{ten}}, 2^{\text{ten}}, \dots, v^{\text{ten}}$ etc. Ecke zusammenstossen. Es ergibt sich so die Gleichung:

$$(2) \quad 2(p-1) = -2n + \sum_{v=1}^{v=E} (e_v - 1).$$

*) Vergl. pag. 69; sowie insbesondere Mathem. Annalen Bd. XXI, pag. 8.

**) pag. 64.

***) Die im Texte gegebene Ableitung von p stimmt materiell mit der in der Functionentheorie zumeist gebrauchten, aber minder übersichtlichen Methode überein, besagtes Fundamentalpolygon, oder die aus ihm abgeleitete geschlossene Fläche durch eine über der J Ebene n -blättrig ausgebreitete Fläche zu ersetzen, welche bei $J = 0, 1, \infty$ gewisse Verzweigungen besitzt.

Hiernach ist das Geschlecht der ausgezeichneten Congruenzgruppe der q^{ten} Stufe

$$p = \frac{(q+2)(q-3)(q-5)}{24}.$$

Bekanntlich besteht nämlich das Fundamentalpolygon in dem letzteren Falle aus $q(q^2 - 1)$ Elementardreiecken, welche in $\frac{q^2 - 1}{2}$ Ecken a ($J = \infty$ entsprechend) zu je $2q$, in $\frac{q(q^2 - 1)}{6}$ Punkten b ($J = 0$ entsprechend) zu je 6, und in $\frac{q(q^2 - 1)}{4}$ Ecken c zu je 4 zusammenstossen.

Dieses vorausgesetzt ist es nun ein Leichtes, zu irgend einer zugehörigen Congruenzgruppe g_n der q^{ten} Stufe das Geschlecht p aus Eigenschaften der zugehörigen Untergruppe G_r zu finden.

Wir gehen vom Fundamentalpolygon F der ausgezeichneten Congruenzgruppe der q^{ten} Stufe aus und lassen aus ihr das Fundamentalpolygon f der betrachteten Congruenzgruppe g_n (deren entsprechende Untergruppe in G G_r sein mag) entstehen. Man bemerke, dass hierbei die $q(q^2 - 1)$ Elementardreiecke von F zu je r zusammengehören, da sie in Folge der Substitutionen der g_n zu einander relativ äquivalent sind. Auch die Ecken a, b, c werden in gewissen Gruppen zusammenfallen. Wenn nun die Gruppe G_r z. B. einen Cyclus G_q enthält, so ist klar, dass die $2q$ Elementardreiecke, welche in jedem der bei dem Cyclus G_q festbleibenden Punkte a zusammentreffen, zu je q als relativ äquivalent zusammenfallen. Also entstehen aus diesen besonderen Ecken a von F keine Punkte von f , in denen mehrere Paare von Elementardreiecken zusammenstiessen*).

Um also alle Ecken a' des Polygons f zu finden, in denen je $2q$ Elementardreiecke zusammenstossen, hat man von der Zahl der Ecken a von F alle jene Ecken a wegzunehmen, welche bei einem in der Gruppe G_r enthaltenen Cyclus G_q ungeändert bleiben, und den Rest durch r zu dividiren.

Ganz ähnlich verhält sich die Sache auch bei den Ecken b und c von F (die $J = 0$ und $J = 1$ resp. entsprechen). Wir erhalten so den folgenden Satz**): *Enthält die Gruppe G_r v_q Cyclen der Periode q , v_3 Cyclen der Periode 3, v_2 Cyclen der Periode 2, so enthält das Polygon f genau*

$$\frac{1}{r} \left(\frac{q^2 - 1}{2} - v_q \cdot \frac{q - 1}{2} \right) \text{ Ecken } a', \text{ in denen je } 2q \text{ Elementardreiecke,}$$

*) Anders ausgedrückt: An diesen Stellen, die, wie alle Punkte a , dem Werthe $J = \infty$ angehören, ist f in Bezug auf J nicht verzweigt.

**) Vergl. Math. Ann. Bd. XXI, pag. 8.

$\frac{1}{r} \left(\frac{q(q^2-1)}{6} - v_3 \cdot \frac{q - \binom{q}{3}}{3} \right)$ Ecken b' , in denen je 6 Elementardreiecke,
 $\frac{1}{r} \left(\frac{q(q^2-1)}{4} - v_2 \cdot \frac{q - \binom{q}{4}}{2} \right)$ Ecken c' , in denen je 4 Elementardreiecke
 zusammenstossen.

Damit ist das Geschlecht des Polygons f und der Congruenzgruppe mit Hülfe der Gleichung (2) bestimmt.

Als Beispiel bestimme ich das Geschlecht einer G_{11} bei $q = 11$, welche einer Ikosaedergruppe G_{60}'' entspricht. Bei $q = 11$ giebt es 60 Punkte a , 220 Punkte b , 330 Punkte c des Polygons F . Bei jedem Cyclus der Periode 11 bleiben 5 Punkte a , bei jedem Cyclus der Periode 3, 4 Punkte b , bei jeder Substitution der Periode 2 aber 6 Punkte c fest. Die Ikosaedergruppe G_{60}'' enthält ferner bekanntlich 0 Cyclen der Periode 11, 10 Cyclen der Periode 3, 15 Cyclen der Periode 2; also ist $v_q = 0$, $v_3 = 10$, $v_2 = 15$ zu setzen. Das Fundamentalpolygon f enthält also 1 Ecke a' , in der 11 Invariantendreiecke, 3 Ecken b' , in denen je 3, 4 Ecken c' , in denen je 2 solcher Dreiecke zusammenstossen. Hieraus aber folgt das bekannte Resultat*): $p = 0$.

§ 4.

Tabelle für das Geschlecht p der Congruenzgruppen q^{ter} Stufe.

Ich füge der Tabelle des § 2 jetzt noch 2 andere Tabellen hinzu. Die erste Tabelle enthält die Werthe von v_q , v_3 und v_2 für die VII in § 2 aufgezählten Gruppenarten, wie sich dieselben aus den Untersuchungen über die Gruppe G ergeben, die zweite das berechnete Geschlecht für die umfassendsten dieser Gruppen.

Tabelle A.

	v_q	v_3	v_2
I.	0	0	0
II. a)	1	0	0
II. b) und c) 4 Fälle:			
1) σ (oder τ) $\equiv 0 \pmod{6}$,	0	1	1
2) σ (oder τ) $\equiv 3 \pmod{6}$,	0	1	0
3) σ (oder τ) $\equiv \pm 2 \pmod{6}$,	0	0	1
4) σ (oder τ) $\equiv \pm 1 \pmod{6}$.	0	0	0

*) F. Klein, Ueber die Erniedrigung der Modulargleichungen, Math. Annalen, Bd. XIV, pag. 423.

	ν_2	ν_3	ν_5
III. 4 Fälle:			
1) $\sigma \equiv 0 \pmod{6}$,	1	q	q
2) $\sigma \equiv 3 \pmod{6}$,	1	q	0
3) $\sigma \equiv \pm 2 \pmod{6}$,	1	0	q
4) $\sigma \equiv \pm 1 \pmod{6}$.	1	0	0
IV. a) und b) 4 Fälle:			
σ' (oder τ') $\equiv 0 \pmod{6}$,	0	1	$\sigma' + 1$
σ' (oder τ') $\equiv 3 \pmod{6}$,	0	1	σ'
σ' (oder τ') $\equiv \pm 2 \pmod{6}$,	0	0	$\sigma' + 1$
σ' (oder τ') $\equiv \pm 1 \pmod{6}$.	0	0	σ'
IV. c).	0	0	3
V.	0	4	3
VI.	0	4	9
VII.	0	10	15

Tabelle (B) für das Geschlecht der umfassendsten der in § 2 aufgezählten Congruenzgruppengattungen.

I.

$$p = \frac{(q+2)(q-3)(q-5)}{24}.$$

II.

$$a) \quad p = \frac{(q-5)(q-7)}{24}.$$

Bei b) und c) sind 4 Fälle zu unterscheiden. Es ist dabei $\sigma = \frac{q-1}{2}$ und $\tau = \frac{q+1}{2}$ gesetzt:

	(b)	(c)
1)	$q \equiv 1 \pmod{12}, \quad p = \frac{q^2 - 5q - 8}{12},$	$p = \frac{q^2 - 7q + 18}{12},$
2)	$q \equiv 5 \pmod{12}, \quad p = \frac{q(q-5)}{12},$	$p = \frac{(q-2)(q-5)}{12},$
3)	$q \equiv 7 \pmod{12}, \quad p = \frac{q^2 - 5q - 2}{12},$	$p = \frac{(q-3)(q-4)}{12},$
4)	$q \equiv 11 \pmod{12}, \quad p = \frac{(q-2)(q-3)}{12},$	$p = \frac{q^2 - 7q + 4}{12}.$

III.

$$i = \frac{q-1}{2}; \quad 4 \text{ Fälle:}$$

$$1) \quad q \equiv 1 \pmod{12}, \quad p = \frac{q-13}{12},$$

$$2) \quad q \equiv 5 \pmod{12}, \quad p = \frac{q-5}{12},$$

$$3) \quad q \equiv 7 \pmod{12}, \quad p = \frac{q-7}{12},$$

$$4) \quad q \equiv 11 \pmod{12}, \quad p = \frac{q+1}{12}.$$

IV.

Dieselben 4 Fälle, wie in II b) und c) und III; es ist $\sigma' = \frac{q-1}{2}$,
 $\tau' = \frac{q+1}{2}$ gesetzt:

(a)	(b)	(c)
1) $p = \frac{(q-1)(q-7)}{24}$,	$p = \frac{q^2 - 10q + 33}{24}$,	$p = \frac{(q-5)(q^2 - q - 24)}{96}$,
2) $p = \frac{(q-3)(q-5)}{24}$,	$p = \frac{(q-5)^2}{24}$,	" ,
3) $p = \frac{(q-1)(q-7)}{24}$,	$p = \frac{(q-3)(q-7)}{24}$,	$p = \frac{(q-7)(q+4)(q-3)}{96}$,
4) $p = \frac{(q-3)(q-5)}{24}$,	$p = \frac{q^2 - 10q + 13}{24}$,	" .

V.

$$p = \frac{q^3 - 6q^2 - 51q + 294 + 32\left(\frac{q}{3}\right) + 18\left(\frac{q}{4}\right)}{288}.$$

Unterscheidet man wieder die 4 Fälle von Nr. III, so kommt:

$$1) \quad p - 3 = \frac{(q-13)(q^2 + 7q + 40)}{288},$$

$$2) \quad p = \frac{(q-5)(q+7)(q-8)}{288},$$

$$3) \quad p = \frac{(q-7)(q^2 + q - 44)}{288},$$

$$4) \quad p - 1 = \frac{(q-11)(q+1)(q+4)}{288}.$$

VI.

$$p = \frac{q^3 - 6q^2 - 87q + 582 + 32\left(\frac{q}{3}\right) + 54\left(\frac{q}{4}\right)}{576},$$

Bei Unterscheidung der bekannten 4 Fälle:

$$\begin{aligned} 1) \quad p - 610 &= \frac{(q - 73)(q^2 + 67q + 4804)}{576}, \\ 2) \quad p - 4 &= \frac{(q - 17)(q^2 + 11q + 100)}{576}, \\ 3) \quad p &= \frac{(q - 7)(q^2 + q - 80)}{576}, \\ 4) \quad p - 13 &= \frac{(q - 23)(q^2 + 17q + 304)}{576}. \end{aligned}$$

VII.

$$p = \frac{q^3 - 6q^2 - 171q + 1446 + 80\left(\frac{q}{3}\right) + 90\left(\frac{q}{4}\right)}{1440}.$$

Bei Unterscheidung der 4 Fälle:

$$\begin{aligned} 1) \quad p - 136 &= \frac{(q - 61)(q^2 + 55q + 3184)}{1440}, \\ 2) \quad p - 11 &= \frac{(q - 29)(q^2 + 23q + 496)}{1440}, \\ 3) \quad p - 2 &= \frac{(q - 19)(q^2 + 13q + 76)}{1440}, \\ 4) \quad p &= \frac{(q - 11)(q^2 + 5q - 116)}{1440}. \end{aligned}$$

§ 5.

Die Hauptmoduln von Primzahlstufe.

Aus den Tabellen des § 4 ist nun unmittelbar ersichtlich, dass für $q > 2$ ausser den Hauptmoduln der 3. und 5. Stufe nur noch Hauptmoduln der siebenten, elften und dreizehnten Stufe existiren.

Für die siebente Stufe insbesondere hat man die folgenden Resultate*):

1) Es giebt 8 gleichberechtigte Hauptmoduln m_7 , welche den 8 Congruenzgruppen g_{24} (II, a in § 2) und den 8 cyklischen Untergruppen G_7 entsprechen.

2) Es giebt acht gleichberechtigte Hauptmoduln m_{21} , welche den 8 Congruenzgruppen g_8 (III in § 2) und den 8 halbmetacyklischen Untergruppen G_{21} entsprechen.

3) Es giebt 28 gleichberechtigte Hauptmoduln m_6 , welche den 28 Congruenzgruppen g_{28} (IV, a) und den 28 Doppelpyramidengruppen G'_6 entsprechen.

*) Ich habe dieselben der Hauptsache nach bereits in meiner Mittheilung an die Münchener Akademie vom Februar 1880 angegeben, cf. Math. Annalen Bd. XVII, pag. 81.

4) *Es giebt 21 gleichberechtigte Hauptmoduln m_8 , welche den 21 Congruenzgruppen g_{21} (IV, b) und den 21 Doppelpyramidengruppen G'_8 entsprechen.*

5) *Es giebt 2 Arten von je 7 gleichberechtigten Hauptmoduln m_4 , welche den 2.7 Congruenzgruppen g_{42} (IV, c) und den 2.7 Untergruppen G'_4 entsprechen.*

6) *Es giebt 2 Arten von je 7 gleichberechtigten Hauptmoduln m_{12} , welche den 2.7 Congruenzgruppen g_{14} (V) und den 2.7 Tetraedergruppen G''_{24} entsprechen.*

7) *Es giebt 2 Arten von je 7 gleichberechtigten Hauptmoduln m_{21} , welche den 2.7 Congruenzgruppen g_7 (VI) und den 2.7 Oktaedergruppen G''_{24} entsprechen.*

Jeder Modul m_{24} ist (vgl. § 2) eine rationale Function 2. Grades eines der Moduln m_{12} , jeder Modul m_{12} wieder eine rationale Function 3. Grades eines Moduls m_4 . Es enthält nämlich jede Gruppe G''_{24} eine G'_{12} , jede G'_{12} eine G'_4 als Untergruppe.

Jeder Modul m_8 ist aus demselben Grunde eine rationale Function 2. Grades eines jeden von 2 Moduln m_4 , und es lassen sich immer gleichzeitig 3 Moduln m_8 durch denselben Modul m_4 rational darstellen. Denn es enthält jede G'_8 2 Gruppen G'_4 , jede G'_4 aber gehört zu 3 Gruppen G'_8 .

Analog folgt:

Jeder Modul m_{24} lässt sich durch jeden von 4 bez. 3 Moduln m_6 bez. m_8 darstellen, und immer je 2 Moduln m_{24} sind rationale Functionen desselben Moduls m_6 oder m_8 .

Jeder Modul m_{21} lässt sich als rationale Function 3. Grades eines Moduls m_7 darstellen. —

Insbesondere mögen wir unter den jedesmaligen gleichberechtigten Moduln je einen in der Art aussuchen, dass unter den zugehörigen Untergruppen G_7 in G'_{21} , G'_6 in G'_{24} , G'_4 in G'_8 und G'_{12} , G'_{12} und G'_8 in G'_{24} enthalten sind. Dann drücken sich die betreffenden Hauptmoduln, deren Anzahl 10 ist ($m_7, m_6, m'_4, m''_4, m_8, m_{21}, m'_{12}, m''_{12}, m'_{24}, m''_{24}$), durch je einen der 4 Hauptmoduln m_7, m_8, m'_4, m''_4 rational aus. Für letztere 4 Moduln habe ich l. c. (Math. Annalen XVII, pag. 81) explicite analytische Formeln angegeben. —

Was die elfte Stufe betrifft, so erhält man nur 2 Arten von je 11 gleichberechtigten Hauptmoduln m_{60} , welche zu den 2.11 Congruenzgruppen g_{11} und den 2.11 Ikosaedergruppen G''_{60} (VII) gehören. Es giebt also nur zwei wesentlich verschiedene Hauptmoduln der 11. Stufe. Es sind dies dieselben Grössen, welche F. Klein bei seiner Untersuchung der Transformation 11. Ordnung (Math. Annalen XV, pag. 533 ff.) mit z bezeichnet hat.

Für die dreizehnte Stufe erhält man:

- 1) 14 gleichberechtigte Hauptmoduln m_{78} , welche den 14 g_{14} (III) und den 14 G'_{78} entsprechen;
- 2) 14 gleichberechtigte Hauptmoduln m_{39} , welche den 14 g_{28} (III) und den 14 G'_{39} entsprechen;
- 3) 14 gleichberechtigte Hauptmoduln m_{26} , welche den 14 g_{42} (III) und den 14 G'_{26} entsprechen.

Unter ihnen können wir dann wieder drei wesentlich verschiedene Hauptmoduln m_{26} , m_{39} , m_{78} in der Art aussuchen, dass sich m_{78} als rationale Function dritten Grades von m_{26} und als Function zweiten Grades von m_{39} darstellt. Der Modul m_{78} ist dieselbe Grösse, welche im 14^{ten} Bande dieser Annalen, pag. 143, Formel (21) daselbst, von F. Klein als τ bezeichnet ist. —

Mit diesen Angaben haben wir den Zielpunkt erreicht, den wir uns in gegenwärtiger Arbeit gesteckt hatten.

Bamberg, den 1. Februar 1883.