16.

Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze, irreductible Congruenzen betreffend (S. 182 Bd. 39 dieses Journals).

(Von Herrn Prof. Dr. *Schönemann* zu Brandenburg a. d. H.)

I. **Aufgabe.** Wenn $a_0, a_1, \dots a_{n-1}$, so wie $b_0, b_1, \dots b_{n-1}$ gegebene ganze Zahlen bedeuten, $fx \equiv 0 \pmod{p}$ eine irreductible Congruenz vom $n$ten Grade und α eine Wurzel der Gleichung $fx \equiv 0$ ist, so ist zu untersuchen, in welchen Fällen sich β als Function von α so bestimmen läfst, dafs es der Congruenz $a_0\alpha + a_1\alpha + \dots a_{n-1}\alpha^{n-1} \equiv b_0\beta + b_1\beta^p + b_2\beta^{p^2} + \dots$ $\dots b_{n-1}p^{n-1}$ genügt, und in welchen Fällen für β verschiedene Functionen von α eintreten können.

Auflösung. Setzt man $a_0\alpha + a_1\alpha + a_2\alpha^2 + \dots a_{n-1}\alpha^{n-1} = (K\alpha)$, so erhält man durch Potenziiren und in Berücksichtigung, dafs $\beta^{p^n} \equiv \beta \pmod{p, \alpha}$ ist, folgendes System von Congruenzen:

$$\begin{array}{l}
b_0\beta + b_1\beta^p + b_2\beta^{p^2} + \dots + b_{n-1}\beta^{p^{n-1}} \equiv (K\alpha) \\
b_{n-1}\beta + b_0\beta^p + b_1\beta^{p^2} + \dots + b_{n-2}\beta^{p^{n-1}} \equiv (K\alpha)^p \\
b_{n-2}\beta + b_{n-1}\beta^p + b_0\beta^{p^2} + \dots + b_{n-3}\beta^{p^{n-2}} \equiv (K\alpha)^{p^2} \\
\dots\dots\dots\dots\dots\dots\dots\dots \\
b_1\beta + b_2\beta^p + b_3\beta^{p^2} + \dots + b_0\beta^{p^{n-1}} \equiv (K\alpha)^{p^{n-1}}.
\end{array}$$

Aus diesen Congruenzen ist nun klar, dafs sich im Allgemeinen β durch $(K\alpha), (K\alpha)^p, \dots (K\alpha)^{p^{n-1}}$, und zwar nur auf eine Weise werde darstellen lassen. Doch würde es unrichtig sein, anzunehmen, dafs dies ohne Ausnahme geschehen könne. Hiezu müfste erst nachgewiesen werden, dafs nicht irgend eine der aufgestellten Congruenzen sich als eine Folge gewisser anderer, oder aber auch mit gewissen andern in Widerspruch stehend ergeben könnte. Im ersten Falle würde es verschiedene Functionem β geben, die der Aufgabe Genüge leisten, im andern keine. Glücklicherweise ist die Form dieser Congruenzen von der Art, dafs sie eine übersichtliche Auflösung gestatten, so dafs man aus derselben die Kennzeichen für die Ausnahme-Fälle wird aufstellen können. Ist nämlich w eine $n$te Wurzel der Einheit und man multiplicirt diese Congruenz mit w^{0i},

die zweite mit w^i, die dritte mit w^{2i}, etc. und addirt sämmtliche Congruenzen, indem man dem i alle Werthe von 0, 1, 2, ... $n-1$ beilegt, so erhält man folgendes System von Congruenzen:

$$(b_0+b_{n-1}+b_{n-2}+\ldots b_1)(\beta+\beta^p+\beta^{p^2}+\ldots\beta^{p^{n-1}}) \equiv (K\alpha)+(K\alpha)^p+\ldots(K\alpha)^{p^{n-1}}$$

$$(b_0+b_{n-1}w+b_{n-1}w+\ldots b_1w^{n-1})(\beta+\beta^p w+\beta^{p^2}w^2+\ldots\beta^{p^{n-1}}w^{n-1}) \equiv (K\alpha)+(K\alpha)^p w+\ldots(K\alpha)^{p^{n-1}}w^{n-1}$$

. . . . . .

$$(b_0+b_{n-1}w^{n-1}+b_{n-2}w^{2(n-1)}+\ldots b_1w^{(n-1)^2})(\beta+\beta^p w^{n-1}+\ldots\beta^{p^{n-1}}w^{(n-1)^2}) \equiv (K\alpha)+(K\alpha)^p w^{n-1}+\ldots(K\alpha)^{p^{n-1}}w^{(n-1)^2}.$$

Diese Congruenzen werden eine und nur eine Auflösung gestatten, wenn $(b_0+b_{n-1}+\ldots b_1)(b_0+b_{n-1}w+\ldots b_1w^{n-1})\ldots(b_0+b_{n-1}w^{n-1}+\ldots b_1w^{(n-1)^2})$ nicht $\equiv 0 \pmod p$ ist. Sobald aber dieser Fall eintritt, ist es zweifelhaft, ob es nur eine Auflösung für β gebe, oder mehrere, oder gar keine. So ist es insbesondere klar, dafs, wenn $(K\alpha)+(K\alpha)^p+\ldots+(K\alpha)^{p^{n-1}}$ nicht $\equiv 0 \pmod{p,\alpha}$ ist, wohl aber $b_0+b_{n-1}+\ldots b_1 \equiv 0 \pmod p$, für β keine Auflösung existiren könne. Ist aber $b_0+b_{n-1}+\ldots b_1$ zugleich mit $(K\alpha)+(K\alpha)^p+\ldots(K\alpha)^{p^{n-1}} \equiv 0 \pmod{p,\alpha}$ und $(b_0+b_{n-1}w+\ldots b_1w^{n-1})\ldots(b_0+b_{n-1}w^{n-1}+\ldots b_1w^{(n-1)^2})$ nicht $\equiv 0 \pmod{p,\alpha}$, so giebt es für β, β^p, ... $\beta^{p^{n-1}}$ nur $n-1$ lineäre Congruenzen, und da man nun die Summe dieser Ausdrücke einer der Zahlen 0, 1, 2, ... $p-1$ congruent setzen kann, so wird es offenbar für β in diesem Falle p verschiedene Auflösungen geben. Zur vollständigen Beantwortung der Frage wird man gelangen, wenn man w als Wurzel der Congruenz $x^n-1 \equiv 0 \pmod p$ ansieht und sowohl α als w als Functionen der Wurzeln einer irreductibeln Congruenz $yx \equiv 0 \pmod p$ auffafst.

Untersuchen wir jetzt die Frage, ob $b_0\beta+b_1\beta^p+\ldots b_{n-1}\beta^{p^{n-1}}$ immer ein vollständiges Restensystem gebe, wenn man für b_0, b_1, ... b_{n-1} alle möglichen Werthe der Zahlen 0, 1, 2, ... $p-1$ setzt. Hier ist zunächst zu bemerken, dafs, wenn n keine Primzahl und n_1 ein Factor von n ist, β von einer irreductibeln Congruenz vom Grade n_1 abhangen kann. Da aber dann von den Werthen β, β^p, ... $\beta^{p^{n-1}}$ je $\frac{n}{n_1}$ zusammenfallen, so kann jenes Restensystem höchstens $p^{\frac{n}{n_1}}$ verschiedene Reste fassen, also nicht vollständig sein, indem das vollständige System p^n Reste in sich schliefst. Wenn aber β von einer Congruenz $n$ten Grades abhangt, so müfste nachgewiesen werden,

dafs, wenn $b_0\beta + b_1\beta^p + \ldots b_{n-1}\beta^{p^{n-1}} \equiv c_0\beta + c_1\beta^p + \ldots c_{n-1}\beta^{p^{n-1}} \pmod{p, \alpha}$ ist, $b_0 \equiv c_0$, $b_1 \equiv c_1$, etc. (mod. p) sein müfste, oder dafs, wenn $m_0\beta + m_1\beta^p + \ldots + m_{n-1}\beta^{p^{n-1}} \equiv 0 \pmod{p, \alpha}$ ist und m_0, $m_1, \ldots m_{n-1}$ bedeuten ganze Zahlen, m_0, m_1, etc. einzeln $\equiv 0$ (mod. p) sein müssen. Dieser Satz kann offenbar wieder nur unter der Beschränkung gelten, dafs $\beta + \beta^p + \ldots \beta^{p^{n-1}}$ nicht $\equiv 0 \pmod{p, \alpha}$ ist. Unter dieser Voraussetzung läfst sich der Satz leicht beweisen, wenn p eine primitive Wurzel der Congruenz $x^n - 1 \equiv 0 \pmod{n}$ und n eine Primzahl ist. In diesem Falle ist $x^n - 1 \equiv 0 \pmod{p}$ eine irreductible Congruenz, und keiner der Factoren $m_0 + m_1 w + \ldots m_{n-1}w^{n-1}$ kann $\equiv 0 \pmod{p, w}$ werden. (S. §. 50. der citirten Abhandlung.)

Setzt man nun in das oben aufgestellte System lineärer Gleichungen 0 statt $K\alpha$, so mufs jeder der Ausdrücke $\beta + \beta^p w + \ldots \beta^{p^{n-1}} w^{n-1} \equiv 0 \pmod{p, \alpha}$ werden. Da nun aber $\beta + \beta^p + \ldots \beta^{p^{n-1}}$ irgend einer ganzen Zahl n (mod. p) congruent werden mufs, so würde man durch Addition aller dieser Gleichungen $n\beta \equiv n \pmod{p, \alpha}$ erhalten; was der Voraussetzung widerspricht, dafs β von einer irreductibeln Congruenz $n$ten Grades abhangt.

Obgleich dieser Satz unter der gemachten Einschränkung wahrscheinlich allgemein richtig ist, so fehlt doch noch der allgemeine Beweis.

II. Es ist $\alpha + w\alpha^p + w^2\alpha^{p^2} + \ldots w^{n-1}\alpha^{p^{n-1}} \equiv w(\alpha^p + w\alpha^{p^2} + \ldots + w^{n-2}\alpha^{p^{n-2}} + w^{n-1}\alpha^{p^n}) \pmod{p, \alpha}$, da $w^n = 1$ und $\alpha^{p^n} \equiv \alpha \pmod{p, \alpha}$ ist. Setzt man nun $\alpha + w\alpha^p + \ldots w^{n-1}\alpha^{p^{n-1}} = f_1(\alpha, w)$, so hat man $f_1(\alpha, w) \equiv w f_1(\alpha^p, w) \equiv w^m f_1(\alpha^{p^m}, w)$, wo m irgend eine ganze Zahl bedeuten kann. Sind nun $w_1, w_2, \ldots w_q$ verschiedene Wurzeln der Einheit, von der Art, dafs $w_1, w_2, \ldots w_q = 1$ ist, so hat man $f_1(\alpha, w_1) f_1(\alpha, w_2) \ldots f_1(\alpha, w_q) = w_1 w_2 \ldots w_q f_1(\alpha^p, w_1) f(\alpha^p, w_2) \ldots f(\alpha^p, w_q) = f_1(\alpha^p, w_1) f(\alpha^p, w_2) \ldots f(\alpha^p, w_q)$. Setzt man $f(\alpha, w_1) f(\alpha, w_2) \ldots f(\alpha, w_q) = \Pi(\alpha, w)$, so ergiebt sich $\Pi(\alpha, w) \equiv \Pi(\alpha^p, w) \ldots \equiv \Pi(\alpha^{p^{n-1}}, w)$. Da sich nun die Summe der letzten Ausdrücke aus den Coëfficienten der Gleichung $fx = 0$ bestimmen läfst, so gilt Dasselbe auch für jeden einzelnen Ausdruck, so lange n nicht ein Vielfaches von p wird. Für diesen Fall ist der gegebene Beweis nicht genügend.

Notiz.

(Von dem Herrn Prof. Dr. *Schönemann* zu Brandenburg a. d. H.)

Herr Dr. ***Eisenstein*** stellt in seiner Abhandlung über die Lemniscatentheilung (im 2ten Hefte Band 39 Seite 166 dieses Journals) den Satz auf, dafs die Gleichung $Fx = 0$ irreductibel sei, wenn der Coëfficient der höchsten Potenz von $x = 1$ und alle übrigen ganzzahligen Coëfficienten durch eine reelle oder complexe Primzahl aufgehen, der letzte aber nicht durch das Quadrat dieser Primzahl theilbar ist. Mit Hülfe dieses Satzes beweiset er die Irreductibilität der Gleichung $\frac{x^p - 1}{x - 1} = 0$, wenn p eine Primzahl ist. Da Herr ***Eisenstein*** ausdrücklich bemerkt, dafs ihm von letzterem Satze nur der Beweis von ***Gaufs*** und von ***Kronecker*** bekannt sei, so sehe ich mich veranlafst, daran zu erinnern, dafs ich bereits im Bande 31 dieses Journals §. 6, in meiner Abhandlung „Grundzüge einer allgemeinen Theorie der höhern Congruenzen etc." den ersten Satz für reelle Primzahlen bewiesen und auch den folgenden aus demselben abgeleitet habe und dafs ferner die von Herrn etc. ***Eisenstein*** angewendete Methode nicht wesentlich von der meinigen verschieden ist. Von dem letztern Satze habe ich übrigens noch einen ganz verschiedenen Beweis im ersten Theile und §. 50 derselben Abhandlung gegeben.

Brandenburg a. d. H., den 14ten December 1849.