11.

Von denjenigen Moduln, welche Potenzen von Primzahlen sind.

(Von Herrn Oberlehrer Dr. *Schönemann* am Gymnasio zu Brandenburg an der Havel.)

(Fortsetzung und Schlufs der Abhandlung Nr. 22. im vorigen Bande.)

§. 51.

Die Begriffe von einfachen und irreductibeln Ausdrücken von x sollen auch auf zusammengesetzte Moduln angewendet werden.

Es läfst sich sogleich übersehen, dafs jeder Ausdruck, in welchem der Coëfficient der höchsten Potenz von x mit dem Modul keinen Factor gemeinschaftlich hat, sich nach demselben dem Producte eines einfachen Ausdrucks und des Coëfficienten der höchsten Potenz congruent setzen lasse. (Vergl. §. 2.)

§. 52.

Lehrsatz. Ist der Modul die m^{te} Potenz einer Primzahl p, und das Product zweier Ausdrücke von x ist $\equiv 0 \pmod{p^m}$, so mufs der zweite Ausdruck $\equiv 0 \pmod{p^n}$ sein, wenn der erste Ausdruck nicht $\equiv 0 \pmod{p}$ ist.

Bezeichnet man also jene beiden Ausdrücke durch $f_1 x$ und $f_2 x$, ist $f_1 x f_2 x \equiv 0 \pmod{p^m}$, und weifs man, dafs $f_1 x$ nicht $\equiv 0 \pmod{p}$ ist, so mufs $f_2 x \equiv 0 \pmod{p^m}$ sein.

Beweis. Zunächst folgt $f_2 x \equiv 0 \pmod{p}$ (§. 4.); daher kann man $f_2 x = p f_3 x$ setzen, wo $f_3 x$ einen Ausdruck von x bedeutet. Da nun $p f_1 x f_3 x \equiv 0 \pmod{p^m}$ ist, so mufs $f_1 x f_3 x \equiv 0 \pmod{p^{m-1}}$ sein. Nun mufs wieder (§. 4.) $f_3 x \equiv 0 \pmod{p}$ sein, wenn m gröfser als 1 ist, und man kann $f_3 x = p f_4 x$ und $f_2 x = p^2 f_4 x$ setzen. Durch fortgesetzte Anwendung derselben Schlufsfolge erhält man zuletzt $f_2 x = p^m f_{2+m} \equiv 0 \pmod{p^m}$.

Zusatz. Ist $ax \cdot bx \equiv cx \cdot dx \pmod{p^m}$, wo ax, bx, cx und dx Ausdrücke von x bedeuten, und weifs man, dafs $ax \equiv cx \pmod{p^m}$ ist, dafs aber diese beiden Ausdrücke nicht $\equiv 0 \pmod{p}$ sind: so mufs auch $bx \equiv dx \pmod{p^m}$ sein. Da nämlich aus obiger Congruenz leicht folgt, dafs $ax(bx - dx) \equiv 0 \pmod{p^m}$ sein müsse, und da nach der Voraussetzung ax nicht $\equiv 0 \pmod{p}$ ist, so mufs $bx - dx \equiv 0 \pmod{p^m}$ oder $bx \equiv dx \pmod{p^m}$ sein.

§. 53.

Lehrsatz. Wenn
$(x^n+a_1x^{n-1}+\cdots+a_n)(A+pFx)\equiv(x^n+b_1x^{n-1}+\cdots+b_n)(A_1+pF_1x)\pmod{p^m}$
ist und $a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n, A$ und A_1 bedeuten ganze Zahlen, von welchen A und A_1 nicht $\equiv 0 \pmod p$ sind, und Fx und F_1x sind Ausdrücke von x: so ist auch $x^n+a_1x^{n-1}+\cdots+a_n\equiv x^n+b_1x^{n-1}+\cdots+b_n \pmod{p^m}$ und $A+pFx\equiv A_1+pF_1x \pmod{p^m}$.

Beweis. Zunächst folgt der Satz für $m=1$ unmittelbar, und man kann daher $x^n+b_1x^{n-1}+b_2x^{n-2}+\cdots b_n=x^n+a_1x^{n-1}+\cdots a_n+p(c_0x^{n-1}+c_1x^{n-2}+\cdots c_{n-1})$ und $A_1=A+pz$ setzen, wo $c_0, c_1, \ldots c_{n-1}$ und z ganze Zahlen bedeuten. Setzt man nun $z+F_1x=F_2x$, so erhält man $(x^n+a_1x^{n-1}+\cdots+a_n)(A+pFx)\equiv(x^n+a_1x^{n-1}+\cdots+a_n+p(c_0x^{n-1}+c_1x^{n-2}+\cdots c_{n-1}))(A+pF_2x) \pmod{p^m}$ und hieraus

$$(x^n+a_1x^{n-1}+\cdots+a_n)(p(Fx-F_2x))$$
$$\equiv p(c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1})(A+pF_2x) \pmod{p^m},$$ und daher
$$(x^n+a_1x^{n-1}+\cdots+a_n)(Fx-F_2x)$$
$$\equiv (c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1})(A+pF_2x) \pmod{p^{m-1}}.$$

Ist nun m gröfser als 1, so findet die letzte Congruenz gewifs auch in Bezug auf den Modul p Statt. Da aber rechts das Glied ausfällt, welches x^n enthält, so mufs das Gleiche auch auf der linken Seite geschehen. Dies kann aber nur erfolgen, wenn $Fx-F_2x\equiv 0 \pmod p$ ist. Setzt man demnach $Fx-F_2x=pF_3x$, so erhält man, da $A+pF_2x$ nicht $\equiv 0 \pmod p$ sein kann, $c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1}\equiv 0 \pmod p$. Setzt man daher den Ausdruck $c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1}=p\varphi x$, wo φx einen Ausdruck von x bedeutet, der den $(n-1)^{\text{ten}}$ Grad nicht übersteigen kann, so erhält man $(x^n+a_1x^{n-1}+\cdots+a_n)F_3x \equiv \varphi x(A+pF_2x) \pmod{p^{m-2}}$ und $x^n+b_1x^{n-1}+\cdots+b_n = x^n+a_1x^{n-1}+\cdots+a_n+p^2\varphi x$, und mithin $x^n+b_1x^{n-1}+\cdots+b_n\equiv x^n+a_1x^{n-1}+\cdots+a_n \pmod{p^2}$.

Ist m gröfser als 2, so mufs auch die Congruenz $(x^n+a_1x^{n-1}+\cdots+a_n)F_3x \equiv \varphi x(A+pF_2x) \pmod p$ Statt finden. Da nun φx von einem geringeren Grade als dem n^{ten} ist, so mufs, wie vorhin, $F_3x\equiv 0 \pmod p$ sein. Man kann daher $F_3x=pF_4x$ setzen, wo F_4x einen Ausdruck von x bedeutet; und hiernach mufs nun auch $\varphi x\equiv 0 \pmod p$ sein, oder es mufs sich $\varphi x=p\varphi_1x$ setzen lassen, wo φx einen Ausdruck von x bedeutet. Hiernach erhält man $x^n+b_1x^{n-1}+\cdots+b_n = x^n+a_1x^{n-1}+\cdots+a_n+p^3\varphi_1x$, und mithin $x^n+b_1x^{n-1}+\cdots+b_n\equiv x^n+a_1x^{n-1}+\cdots+a_n \pmod{p^3}$.

Durch fortgesetzte Anwendung derselben Schlüsse beweiset man zunächst, dafs $x^n + a_1 x^{n-1} + \cdots + a_n \equiv x^n + b_1 x^{n-1} + \cdots + b_n \pmod{p^m}$ sei. Nachdem dies bewiesen ist, folgt auch, dafs $A + pFx \equiv A_1 + pF_1 x \pmod{p^m}$ ist (§. 52. Zus.).

§. 54.

Lehrsatz. Jeder Ausdruck von der Form $a_0 x^\nu + a_1 x^{\nu-1} + a_2 x^{\nu-2} + \cdots + a_{\nu-n} x^n + a_{\nu-n+1} x^{n-1} + \cdots + a_\nu$, in welchem sämmtliche Coëfficienten a_0, a_1, a_2, $\ldots$ $a_{\nu-n-1}$ nach dem Modul p congruent 0 sind, $a_{\nu-n}$ aber nicht congruent 0 nach dem Modul p ist, läfst sich nach dem Modul p^m einem Product von der Form $(x^n + b_1 x^{n-1} + \cdots + b_n)(A + pFx)$ congruent setzen, wo b_1, b_2, $\ldots$ b_n und A ganze Zahlen sind, Fx aber einen Ausdruck vom Grade $\nu - n$ bedeutet.

Beweis. Man bestimme $\beta_1, \beta_2, \ldots \beta_n$ so, dafs $a_{\nu-n} x^n + a_{\nu-n+1} x^{n-1} + \cdots a_\nu \equiv a_{\nu-n}(x^n + \beta_1 x^{n-1} + \cdots \beta_n) \pmod{p}$ wird (§. 2.). Nun giebt es offenbar p^{m-1} Zahlen, die nach dem Modul p einer gegebenen Zahl, etwa β_1, congruent, nach dem Modul p^m aber verschieden sind; diese Zahlen sind nämlich β_1, $\beta_1 + p$, $\beta_1 + 2p$, $\ldots$ $\beta_1 + (p^{m-1} - 1)p$. Da nun der Ausdruck $x^n + \beta_1 x^{n-1} + \ldots + \beta_n$, n Coëfficienten β_1, β_2, $\ldots$ β_n hat, so folgt leicht aus der Combinationslehre, dafs es $p^{(m-1)n}$ einfache Ausdrücke geben wird, die mit $x^n + \beta_1 x^{n-1} + \cdots \beta_n$ nach dem Modul p congruent und die unter sich nach dem Modul p^m sämmtlich verschieden sein werden. Die Totalität dieser Ausdrücke wollen wir die erste Classe nennen.

Setzt man für A irgend eine unveränderliche Zahl, die $\equiv a_{\nu-n} \pmod{p}$ ist, so giebt es so viele Ausdrücke von der Form $A + pFx$, die nach dem Modul p^m verschieden sind, als Ausdrücke, die nach dem Modul p congruent 0 und nach dem Modul p^m verschieden sind. Da aber Fx im Allgemeinen ein vielfacher Ausdruck vom Grade $\nu - n$ ist, also $\nu - n + 1$ veränderliche Coëfficienten in sich schliefst, so folgt, wie vorhin, dafs es $p^{(m-1)(\nu-n+1)}$ Ausdrücke geben werde, die nach dem Modul p mit $A + pFx$ congruent sind, die aber nach dem Modul p^m verschieden sind. Die Totalität dieser Ausdrücke wollen wir die zweite Classe nennen.

Offenbar kann man nun $p^{(m-1)n} \cdot p^{(m-1)(\nu-n+1)} = p^{(m-1)(\nu+1)}$ Producte bilden, die einen Factor aus der ersten Classe und einen aus der zweiten Classe in sich schliefsen. Alle diese Producte werden (§. 53.) nach dem Modul p^m verschieden, aber offenbar nach dem Modul p congruent sein. Nun giebt es aber im Ganzen nur $p^{(m-1)(\nu+1)}$ Ausdrücke, die mit

$$a_0 x^\nu + a_1 x^{\nu-1} + a_2 x^{\nu-2} + \cdots + a_{\nu-n} x^n + \cdots + a_\nu$$

nach dem Modul p congruent, aber nach dem Modul p^m unter sich verschie-

schieden sind: es mufs also auch dieser Ausdruck sich einem Product zweier Factoren aus der ersten und zweiten Classe congruent setzen lassen.

§. 55.

Lehrsatz. Ist das Product eines Ausdrucks, der nicht $\equiv 0 \pmod{p}$ ist, und eines einfachen, nach dem Modul p^m irreductibeln Ausdrucks dem Producte zweier andern Ausdrücke von x nach demselben Modul congruent, so hat einer derselben den irreductibeln Ausdruck nach dem Modul p^m zum Divisor, wenn der andre Ausdruck sich nicht durch den irreductiblen Ausdruck in Bezug auf den Modul p dividiren läfst.

Beweis. Ist der irreductible Ausdruck vom 1^{ten} Grade, so läfst sich der Beweis wie in §. 5. führen.

Wir wollen nun voraussetzen, der Satz sei bis zu dem Grade n bewiesen, und zeigen, er gelte auch für den Grad $n+1$. Es sei demnach φx ein nach dem Modul p^m irreductibler, einfacher Ausdruck vom Grade $n+1$ und $\varphi x f x \equiv Ax Bx \pmod{p^m}$, und fx sei nicht $\equiv 0 \pmod{p}$. Ferner bezeichne man den algebraischen Quotienten, den man erhält, wenn man Bx durch φx dividirt, durch Qx, und den Rest, welcher den n^{ten} Grad nicht überschreiten kann, durch Rx, so erhält man $\varphi x(fx - Ax\,bx) \equiv Ax\,Rx \pmod{p^m}$. Wäre nun Rx nicht $\equiv 0 \pmod{p}$, so kann man $Rx \equiv gx(h+pFx) \pmod{p^m}$ setzen, wo gx einen einfachen Ausdruck von x anzeigt, Fx irgend einen Ausdruck von x, und h eine ganze Zahl, die nicht $\equiv 0 \pmod{p}$ ist, und wo die Summe der Zahlen, welche die Grade von gx und Fx angeben, gleich dem Grade von Rx ist (§. 54.). Man erhält nun $\varphi x(fx - Ax\,Qx) \equiv Ax \cdot gx(h+pFx) \pmod{p^m}$. Da aber gx nur irreductible einfache Factoren von einem geringern Grade als dem $(n+1)^{\text{ten}}$ einschliefsen kann, so müssen diese auch in $fx - Ax \cdot Qx$ enthalten sein, indem φx irreductibel ist. Setzt man nun $fx - Ax \cdot Qx \equiv gx\,Q_1x \pmod{p^m}$, so erhält man leicht $\varphi x \cdot Q_1x \equiv Ax(h+pFx) \pmod{p^m}$. Da aber nach der Voraussetzung φx und fx nicht $\equiv 0 \pmod{p}$ sind, so kann auch Ax nicht $\equiv 0 \pmod{p}$ sein. Man kann daher $Ax \equiv A_1x(h_1+pF_1x) \pmod{p^m}$ setzen, wo F_1x ein Ausdruck von x, A_1x ein einfacher Ausdruck von x, und h_1 eine Zahl ist, die nicht $\equiv 0 \pmod{p}$ ist. Hieraus erhält man $\varphi x\,Q_1x \equiv A_1x(h_1+pF_1x)(h+pFx) \pmod{p^m}$. Da aber Q_1x auch nicht $\equiv 0 \pmod{p}$ sein kann, so kann man $Q_1x \equiv Q_2x(h_2+pF_2x) \pmod{p^m}$ setzen, wo Q_2x ein einfacher Ausdruck, und h_2 nicht $\equiv 0 \pmod{p}$ ist. Daraus ergiebt sich

$\varphi x\, Q_2 x(h_2+pF_2x) \equiv A_1x(h_1+pF_1x)(h+pFx) \pmod{p^m}$. Da nun $\varphi x\, Q_2 x$ und A_1x einfache Ausdrücke, und h, h_1 und h_2 nicht $\equiv 0 \pmod{p}$ sind, so folgt leicht, dafs $\varphi x\, Q_2 x \equiv A_1 x \pmod{p^m}$ (§. 53.) und dafs mithin φx ein Factor von $A_1 x$ und daher auch von Ax in Bezug auf den Modul p^m sei.

§. 56.

Zwei Ausdrücke derselben Wurzel α eines nach dem Modul p^m irreductiblen einfachen Ausdrucks fx sollen auch hier nach dem Modul p^m, α congruent heifsen, wenn sich der eine von ihnen als eine Summe des andern und eines p^mfachen Ausdrucks dieser Wurzel darstellen läfst.

Es folgt dann, wie in §. 14., dafs, wenn $\varphi\alpha \equiv \psi\alpha \pmod{p^m, \alpha}$ ist, auch fx in Bezug auf den Modul p^m ein Theiler von $\varphi x - \psi x$ sein mufs; und umgekehrt.

§. 57.

Lehrsatz. Wird ein Ausdruck von α, der nicht $\equiv 0 \pmod{p, \alpha}$ ist, in einen zweiten Ausdruck von α multiplicirt, so kann das Product nicht $\equiv 0 \pmod{p^m, \alpha}$ werden, wenn nicht der zweite Ausdruck $\equiv 0 \pmod{p^m, \alpha}$ ist.

Gesetzt $\varphi\alpha$ sei ein Ausdruck von α, der nicht $\equiv 0 \pmod{p, \alpha}$ ist, und $\varphi\alpha \cdot \psi\alpha \equiv 0 \pmod{p^m, \alpha}$, so ist zu zeigen, dafs $\psi\alpha \equiv 0 \pmod{p^m, \alpha}$ ist.

Beweis. Da $\varphi\alpha \cdot \psi\alpha \equiv 0 \pmod{p^m, \alpha}$ ist, so mufs $\varphi x \cdot \psi x$ durch den einfachen und in Bezug auf den Modul p^m irreductibeln Ausdruck fx dividirbar sein. Man kann also $\varphi x \cdot \psi x \equiv fx \cdot qx \pmod{p^m}$ setzen, wo qx ein Ausdruck von x ist. Setzt man nun $\varphi x = fx \cdot Qx + Rx$, wo Qx den Quotienten bedeutet, den man bei der Division von φx durch fx erhält, und Rx den Rest: so kann Rx nicht $\equiv 0 \pmod{p}$ sein, weil sonst $\varphi\alpha \equiv 0 \pmod{p, \alpha}$ wäre. Da also φx in Bezug auf den Modul p nicht durch fx theilbar ist, so mufs ψx in Bezug auf den Modul p^m durch fx theilbar sein (§. 52.). Hieraus folgt aber $\psi\alpha \equiv 0 \pmod{p^m, \alpha}$.

§. 58.

Lehrsatz. Ist das Product zweier einfacher Ausdrücke von x dem Product zweier anderer einfacher Ausdrücke von x nach dem Modul p^m congruent: haben ferner die Factoren eines solchen Products nach dem Modul p keinen gemeinschaftlichen Factor, und sind die Factoren des einen Products denen des andern nach dem Modul p congruent: so müssen sie auch nach dem Modul p^m congruent sein.

Bedeuten also fx, f_1x, gx und g_1x Ausdrücke von x, und ist $fx \equiv f_1x \pmod{p}$ und $gx \equiv g_1x \pmod{p}$, ferner $fx \cdot gx \equiv f_1x \cdot g_1x \pmod{p^m}$,

so mufs auch $fx \equiv f_1 x \pmod{p^m}$ und $gx \equiv g_1 x \pmod{p^m}$ sein, wenn fx und gx nach dem Modul p keinen gemeinschaftlichen Factor haben.

Beweis. Zum Beweise setze man $f_1 x = fx + p\varphi x$ und $g_1 x = gx + p\gamma x$, wo φx und γx Ausdrücke von x bedeuten, so ist

$$fx \cdot gx \equiv (fx + p\varphi x)(gx + p\gamma x) \pmod{p^m}.$$

Zunächst bemerke man, dafs $p\varphi x$ und $p\gamma x$ von geringerem Grade sein müssen, als $f_1 x$ und $g_1 x$ oder fx und gx, weil diese vier Ausdrücke nach der Voraussetzung einfach sind. Wäre nun α eine Wurzel eines nach dem Modul p^m irreductibeln einfachen Ausdrucks von x, der nach demselben Modul ein Factor von fx ist, und selbst ex heifsen mag: so folgt aus der Congruenz $fx \cdot gx \equiv (fx + p\varphi x)(gx + p\gamma x) \pmod{p^m}$ die folgende: $0 \equiv p\varphi\alpha(g\alpha + p\gamma\alpha) \pmod{p^m, \alpha}$. Da aber fx und gx nach dem Modul p keinen gemeinschaftlichen Factor haben, so kann $g\alpha$ nicht $\equiv 0 \pmod{p, \alpha}$ sein, und es folgt (§. 57.), dafs $p\varphi\alpha \equiv 0 \pmod{p^m, \alpha}$ sei, und daher, dafs $p\varphi x$ den Factor ex in Bezug auf den Modul p^m in sich schliefse (§. 56.). Setzt man daher $fx \equiv ex \cdot f_2 x \pmod{p^m}$ und $p\varphi x \equiv pex \cdot \varphi_2 x \pmod{p^m}$, so leitet man durch Division mit ex aus der obigen Congruenz nach (§. 52. Zus.) leicht die Congruenz $f_2 x \cdot gx \equiv (f_2 x + p\varphi_2 x)(gx + p\gamma x) \pmod{p^m}$ her. Nun folgt aber wieder, dafs $p\varphi_2 x$ in Bezug auf den Modul p^m jeden einfachen Factor mit $f_2 x$ gemeinschaftlich haben müsse. Durch fortgesetzte Schlüsse derselben Art beweiset man, dafs $p\varphi x$ dieselben Factoren in Bezug auf den Modul p^m enthalte, wie fx. Dies geht aber nur an, wenn $p\varphi x \equiv 0 \pmod{p^m}$ ist, weil es von einem geringeren Grade als fx ist. Ist aber $p\varphi x \equiv 0 \pmod{p^m}$, so ist $f_1 x \equiv fx \pmod{p^m}$, und ebenso $g_1 x \equiv gx \pmod{p^m}$.

§. 59.

Lehrsatz. Ist irgend ein einfacher Ausdruck von x nach dem Modul p in zwei einfache Factoren zerlegbar, die nach demselben Modul keinen gemeinschaftlichen Divisor haben: so ist dieser Ausdruck auch nach dem Modul p^m, ***aber nur auf eine Weise,*** in zwei Factoren zerlegbar, welche jenen beiden ersten nach dem Modul p congruent sind.

Bedeuten also Fx, fx, $f_1 x$, Qx und $Q_1 x$ einfache Ausdrücke von x, ist $Fx \equiv fx\,Qx \pmod{p}$, und haben fx und Qx keinen gemeinschaftlichen Factor nach dem Modul p, so läfst sich auf eine, ***aber nur auf eine*** Weise, $Fx \equiv f_1 x\,Q_1 x \pmod{p^m}$ setzen, so dafs $f_1 x \equiv fx \pmod{p}$ und $Q_1 x \equiv Qx \pmod{p}$ wird.

Beweis. Es sei fx vom Grade n, so giebt es $p^{(m-1)n}$ verschiedene einfache Ausdrücke nach dem Modul p^m, die, nach dem Modul p genommen, mit fx congruent werden. Bezeichnet nämlich a_1 irgend einen Coëfficienten von fx, so ist die Reihe der Ausdrücke a_1, a_1+p, a_1+2p, ... $a_1+(p^{m-1}-1)p$ congruent, aber nach dem Modul p^m verschieden. Da also in fx an die Stelle jedes Coëfficienten p^{m-1} verschiedene Werthe treten können, wenn man statt p den Modul p^m einführt, und da fx, aufser dem Coëfficienten der höchsten Potenz von x, welcher 1 ist, n Coëfficienten hat, so kann dieser Ausdruck $p^{(m-1)n}$ Werthe annehmen, die nach dem Modul p^m verschieden, aber nach dem Modul p congruent sind. Ist nun Qx vom Grade ν, so kann dieser Ausdruck nach dem Modul p^m ebenfalls $p^{(m-1)\nu}$ verschiedene Werthe erhalten. Multiplicirt man einen Ausdruck von fx mit einem Ausdruck von Qx, so erhält das Product den Grad $n+\nu$. Man kann aber wie vorhin schliefsen, dafs es $p^{(m-1)(n+\nu)}$ einfache Ausdrücke nach dem Modul p^m geben werde, die nach dem Modul p mit jenem Product, oder auch mit Fx congruent und nach dem Modul p^m unter sich verschieden sind. Nun giebt es $p^{(m-1)n}$ Ausdrücke, die an die Stelle von fx, und $p^{(m-1)\nu}$ Ausdrücke, die an die Stelle von Qx treten können: also kann man offenbar $p^{(m-1)n}\cdot p^{(m-1)\nu}=p^{(m-1)(n+\nu)}$ Producte bilden, deren Factoren fx und Qx nach dem Modul p beide congruent und nach dem Modul p^m nicht beide congruent sind. Da alle diese Producte auch nach dem Modul p^m verschieden sein müssen, weil ihre beiden Factoren nach der Voraussetzung keinen gemeinschaftlichen Theiler in Bezug auf den Modul p einschliefsen (§. 54.) und es überhaupt nur $p^{(m-1)(n+\nu)}$ verschiedene Ausdrücke nach dem Modul p^m giebt, die mit Fx congruent werden, so folgt, dafs jeder dieser Ausdrücke, also auch Fx, sich nach dem Modul p^m auf eine Weise in zwei Factoren zerfällen lasse, die nach dem Modul p mit fx und Qx congruent werden.

§. 60.

Aus dem vorigen Paragraph ergiebt sich, dafs es bei einer Untersuchung über die Möglichkeit der Zerfällung gegebener Ausdrücke von x nach dem Modul p^m nur darauf ankommt, solche Ausdrücke zu untersuchen, die nach dem Modul p Potenzen von irreductiblen Ausdrücken sind. Denn es mufs jeder Ausdruck, der nach dem Modul p^m irreductibel ist, auch nach dem Modul p irreductibel, oder die Potenz eines irreductibeln Ausdrucks sein.

Demnach ergiebt sich hier ganz naturgemäfs folgende Aufgabe:

§. 61.

Aufgabe. Zu untersuchen, ob die Potenz eines nach dem Modul p irreductibeln Ausdrucks, nach dem Modul p^m irreductibel sei, oder nicht.

Da es indessen scheint, als wenn die Lösung dieser Aufgabe im Allgemeinen sich nicht einfach geben lasse, so soll sie auf den Modul p^2 eingeschränkt und es soll zunächst untersucht werden, in welchem Fall der Ausdruck $(x-a)^n+pFx$, wo a eine ganze Zahl und Fx einen Ausdruck von x bedeutet, nach diesem Modul zerfällbar sei, oder nicht.

Nach dem Modul p hat $(x-a)^n+pFx$ nur Factoren von der Form $(x-a)^m$, wo a und m ganze Zahlen bedeuten (§. 6.); es mufs daher, wenn $(x-a)^n+pFx$ nach dem Modul p^2 zerfällbar ist, jeder der Factoren die Form $(x-a)^m+pRx$ haben; wo Rx einen Ausdruck von x bedeutet. Es sei also $(x-a)^n+pFx \equiv [(x-a)^m+pRx][(x-a)^q+pQx]$ (mod. p^2), wo Qx ebenfalls einen Ausdruck von x, und q eine ganze Zahl bedeutet. Setzt man nun $x=a$, so erhält man offenbar $pFa \equiv 0$ (mod. p^2) und daher $Fa \equiv 0$ (mod. p). Es mufs also Fx nach dem Modul p den Factor $x-a$ haben, und man darf daher den Satz aussprechen: *dafs $(x-a)^n+pFx$ nach dem Modul p^2 irreductibel sein werde, wenn Fx nach dem Modul p nicht den Factor $x-a$ in sich schliefst.* Übrigens folgt leicht, dafs die Erfüllung dieser Bedingung hinreicht, um $(x-a)^n+pFx$ nach dem Modul p^2 zerfällbar zu machen.

Wenden wir das erhaltene Resultat auf den Ausdruck $\frac{x^n-1}{x-1}$ an, wo n eine Primzahl bedeutet. Es ist für diesen Fall $x^n-1 \equiv (x-1)^n$ (mod. n), und man erhält also

$$\frac{x^n-1}{x-1} = x^{n-1}+x^{n-2}+\cdots+x+1 = (x-1)^{n-1}+nFx.$$

Für $x=1$ erhält man $n=nF(1)$ und daher $F(1)=1$, und nicht $\equiv 0$ (mod. n). *Hieraus folgt, dafs $\frac{x^n-1}{x-1}$ nach dem Modul n^2 stets irreductibel ist, wenn n eine Primzahl bedeutet; mithin mufs dieser Ausdruck gewifs in algebraischer Beziehung irreductibel sein.*

Die Leichtigkeit des Beweises dieses Satzes ist auffallend, da derselbe in den „Disquisitiones" mit einem viel gröfsern Aufwande von Scharfsinn, und dennoch viel umständlicher geführt ist. (Vergl. §. 50. Zus. 2.)

Bedeutet nun fx einen Ausdruck, der nach dem Modul p irreductibel ist, so ist jetzt die Bedingung zu finden, unter welcher $(fx)^n+pFx$ nach

dem Modul p^2 irreductibel sei, oder nicht. Da $(fx)^n+pFx$ nach dem Modul p nur Factoren von der Form $(fx)^m$ haben kann, so mufs jeder Factor von $(fx)^n+pFx$ in Bezug auf den Modul p^2 die Form $(fx)^m+pRx$ haben. Setzt man also $(fx)^n+pFx \equiv [(fx)^m+pRx][(fx)^q+pQx]$ (mod. p^2), und α eine Wurzel von fx, so erhält man $pF\alpha \equiv 0$ (mod. p^2, α), und daher $F\alpha \equiv 0$ (mod. p, α). ***Soll demnach*** $(fx)^n+pFx$ ***nach dem Modul*** p^2 ***zerfällbar sein, so mufs*** $F\alpha \equiv 0$ (mod. p, α) ***und folglich*** fx ***in Bezug auf den Modul*** p ***ein Factor von*** Fx ***sein*** *). Dafs diese Bedingung für die Zerfällbarkeit auch hinreiche, ist ebenfalls leicht zu sehen.

§. 62.

Lehrsatz. Ist fx ein einfacher irreductibler Ausdruck in Bezug auf den Modul p, und vom n^{ten} Grade, und $\varphi\alpha$ irgend ein Ausdruck einer Wurzel desselben, der nicht $\equiv 0$ (mod. p, α) ist: so ist stets $(\varphi\alpha)^{p^{m-1}(p^n-1)} \equiv 1$ (mod. p^m, α); oder: Die $p^{m-1}(p^n-1)^{\text{te}}$ Potenz jedes Ausdrucks der Wurzel einer nach dem Modul p irreductibeln einfachen Congruenz ist nach dem Modul (p^m, α) congruent 1, wenn der Ausdruck selbst nicht $\equiv 0$ (mod. p, α) ist.

Beweis. Es ist $(\varphi\alpha)^{p^n-1} \equiv 1$ (mod. p, α) (§. 19.). Schreibt man diese Congruenz als Gleichung, so erhält man $(\varphi\alpha)^{p^n-1} = 1+pR\alpha$, wo $R\alpha$ einen Ausdruck von α bedeutet. Erhebt man beide Seiten der Gleichung zur Potenz p^{m-1} und bedenkt, dafs $(1+pR\alpha)^{p^{m-1}} \equiv 1$ (mod. p^m, α) ist (wie leicht aus der Entwicklung nach dem binomischen Lehrsatze folgt), so erhält man $(\varphi\alpha)^{p^{m-1}(p^n-1)} \equiv 1$ (mod. p^m, α).

Zusatz. Da $fx \equiv (x-\alpha)(x-\alpha^p)\ldots(x-\alpha^{p^{n-1}})$ (mod. p, α) ist (§. 18), so erhält man, wenn man diese Congruenz als Gleichung schreibt:

$$fx = (x-\alpha)(x-\alpha^p)\ldots(x-\alpha^{p^{n-1}})+pF(x, \alpha),$$

wo $F(x, \alpha)$ einen Ausdruck von x bedeutet, dessen Coëfficienten Ausdrücke von α sind. Erhebt man beide Seiten dieser Gleichung zur $(p^{m-1})^{\text{ten}}$ Potenz und schliefst wie vorher, so erhält man

$$(fx)^{p^{m-1}} \equiv \left[(x-\alpha)(x-\alpha^p)\ldots(x-\alpha^{p^{n-1}}\right]^{p^{m-1}} \text{ (mod. } p^m, \alpha).$$

Man kann diese Formel als die allgemeinere der ersten Formel in (§. 18.) an-

*) Setzt man nämlich $Fx = fx \cdot qx + rx$, wo qx den algebraischen Quotienten bedeutet, den man erhält, wenn man Fx durch fx dividirt, und rx den Divisions-Rest: so ist offenbar $F\alpha = r\alpha$. Da nun $F\alpha \equiv 0$ (mod. p, α) ist, so mufs auch $r\alpha \equiv 0$ (mod. p, α) sein. Dies kann aber nur geschehen, wenn rx ein $p$facher Ausdruck ist. In diesem Falle ist dann aber fx in Bezug auf den Modul p ein Theiler von Fx, wie oben vorausgesetzt wird.

sehen. Indessen wird die wahre Bedeutung jener Formel für den Modul (p^m, α) erst in Folgendem gezeigt werden.

§. 63.

Wenn fx ein einfacher und nach dem Modul p irreductibler Ausdruck ist, dessen Wurzeln $\alpha, \alpha_1, \alpha_2, \ldots \alpha_{n-1}$ sind; ferner φx irgend einen andern Ausdruck von x bezeichnet, und $(z-\varphi\alpha)(z-\varphi\alpha_1)\ldots(z-\varphi\alpha_{n-1})$, welches gleich Fz gesetzt werden mag, ebenfalls nach dem Modul p irreductibel ist, und man hat $D\varphi x = fx\cdot qx + p^m rx$, wo $D\varphi x$ einen Ausdruck von φx, qx und rx aber Ausdrücke von x bedeuten: so kann man auch $Dz = Fz\cdot Qz + p^m Rz$ setzen, wo Qz und Rz ebenfalls Ausdrücke von z bezeichnen. Oder, wenn $D\varphi\alpha \equiv 0 \pmod{p^m, \alpha}$ ist, so mufs auch $D\varphi\alpha \equiv 0 \pmod{p^m, \varphi\alpha}$ sein, wenn Fz oder $(z-\varphi\alpha)(z-\varphi\alpha_1)\ldots(z-\varphi\alpha_{n-1})$ nach dem Modul p irreductibel ist.

Beweis. Man setze $Dz = Fz\,Q_1 z + R_1 z$, wo $Q_1 z$ den algebraischen Quotienten und $R_1 z$ den Rest bedeutet, welchen man erhält, wenn man Dz durch Fz dividirt. Da nun $D\varphi x = fx\cdot qx + p^m rx$ und daher $D\varphi\alpha = p^m r\alpha$, $D\varphi\alpha_1 = p^m r\alpha_1$, $\ldots$ $D\varphi\alpha_{n-1} = p^m r\alpha_{n-1}$ ist, so folgt, dafs $N(D_F) = D\varphi\alpha\, D\varphi\alpha_1 \ldots D\varphi\alpha_{n-1} = p^{n\cdot m} r\alpha\, r\alpha_1 \ldots r\alpha_{n-1}$ sein werde. Es ist mithin offenbar $N(D_F) \equiv 0 \pmod{p}$, und daher Fz ein Theiler von Dz in Bezug auf den Modul p (§. 11.). Man kann folglich $R_1 z = pR_2 z$ setzen, wo $R_2 z$ einen Ausdruck von z bedeutet. Dann erhielte man aber $N(D_F) = N(pR_{2_F}) = p^n NR_{2_F} = p^{n\cdot m} r\alpha_1 r\alpha_2 \ldots r\alpha_{n-1}$ und mithin

$$N(R_{2_F}) = p^{n(m-1)} r\alpha\, r\alpha_1 \ldots r\alpha_{n-1}.$$

Ist nun $m > 1$, so mufs $N(R_{2_F})$ ebenfalls $\equiv 0 \pmod{p}$ und daher $R_2 z$ von der Form $pR_3 z$ sein, wo $R_3 z$ einen Ausdruck von z bedeutet. Hieraus folgt $R_1 z = p^2 R_3 z$ und $Dz = Fz\cdot Q_1 z + p^2 R_3 z$. Setzt man diese Schlüsse fort, so erhält man $Dz = Fz\cdot Q_1 z + p^{m-1} R_m z$. Dann erhielte man aber $N(R_{1_F}) = N(p^{m-1} R_{m_F}) = p^{n(m-1)} N(R_{m_F}) = p^{n\cdot m} r\alpha_1 r\alpha_2 \ldots r\alpha_{n-1}$ und mithin

$$NR_{m_F} = p^n r\alpha\, r\alpha_1 r\alpha_2 \ldots r\alpha_{n-1}.$$

Hiernach wäre schliefslich $N(R_{m_F}) = 0 \pmod{p}$ und $R_m z = pR_{m+1} z$, und daher $Dz = Fz\,Q_1 z + p^m R_{m+1} z$. Setzt man nun $Qz = Q_1 z$ und $Rz = R_{m+1} z$, so ist der Satz bewiesen.

§. 64.

Lehrsatz. Ist fx ein einfacher Ausdruck vom Grade n, und in Bezug auf den Modul p irreductibel: ist ferner Fz ebenfalls ein einfacher Ausdruck

von x, dessen Wurzeln die $(p^{m-1})^{\text{ten}}$ Potenzen der Wurzeln von fx sind: so ist stets:

$$Fx \equiv (x-\beta)(x-\beta^p)(x-\beta^{p^2}) \ldots (x-\beta^{p^{n-1}}) \pmod{p^m, \beta};$$

wenn β eine Wurzel von Fx ist.

Beweis. Da $fx \equiv Fx \pmod{p}$ sein mufs (§. 13.), so folgt, dafs auch Fx, und somit auch Fx zugleich mit fx nach dem Modul p irreductibel sein mufs. Ist nun α eine Wurzel von fx, so erhält man $\alpha^{p^{m-1}(p^n-1)} - 1 \equiv 0 \pmod{p^m, \alpha}$ (§. 58.). Hieraus folgt, dafs fx in Bezug auf den Modul p^m ein Factor von $x^{p^{m-1}(p^n-1)} - 1$ ist (§. 52.). Setzt man nun $x^{p^{m-1}} = z$, so erhält man $x^{p^{m-1}(p^n-1)} - 1 = z^{p^n-1} - 1$. Beide Ausdrücke treten an die Stelle von $D\varphi x$ und Dz im vorigen Paragraphen. Da man nun $x^{p^{m-1}(p^n-1)} - 1 = fx \cdot qx + p^m rx$ setzen kann, so folgt auch, dafs $z^{p^n-1} - 1 = Fz \cdot Qz + p^m Rz$, oder dafs Fz in Bezug auf den Modul p^m ein Divisor von $z^{p^n-1} - 1$ sei. Aber das Product sämmtlicher, nach dem Modul p verschiedenen irreductiblen Ausdrücke von x, deren Grad in n aufgeht, ist $\equiv z^{p^n-1} \pmod{p}$ (§. 45.): also können Fz und Qz in Bezug auf den Modul p keinen gemeinschaftlichen Factor haben. Setzt man in die letzte Gleichung statt z den Werth β und bedenkt, dafs $F\beta = 0$ ist, so erhält man $\beta^{p^n-1} - 1 = p^m R\beta$ oder $\beta^{p^n-1} \equiv 1 \pmod{p^m, \beta}$, und hieraus $(\beta^p)^{(p^n-1)} \equiv 1 \pmod{p^m, \beta}$ oder $(\beta^p)^{(p^n-1)} - 1 \equiv 0 \pmod{p^m, \beta}$. Setzt man aber in dieselbe Gleichung statt z den Werth β^p, so erhält man $(\beta^p)^{(p^n-1)} - 1 = F\beta^p \, Q\beta^p + p^m R\beta^p$, und mithin, da $(\beta^p)^{(p^n-1)} - 1 \equiv 0 \pmod{p^m, \beta}$ ist, $F\beta^p \, Q\beta^p \equiv 0 \pmod{p^m, \beta}$. Da indessen der Ausdruck, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von Fz sind, mit Fz nach dem Modul p congruent ist, und Qz mit Fz keinen gemeinschaftlichen Factor nach dem Modul p hat, so kann Qp^p nicht $\equiv 0 \pmod{p, \beta}$ sein: es mufs mithin $Fp^p \equiv 0 \pmod{p^m, \beta}$ sein (§. 57.). Ebenso läfst sich beweisen, dafs jeder der Ausdrücke $F\beta^{p^2}$, $F\beta^{p^3}$, $\ldots \equiv 0 \pmod{p^m, \beta}$ sei. Hiermit ist die Grundlage des Beweises gewonnen, und derselbe kann nun ganz ähnlich wie im §. 18. zu Ende geführt werden.

Zusatz 1. Man kann auch behaupten, dafs der einfache Ausdruck, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von Fz sind, mit Fz nach dem Modul p^m congruent sein müsse. Man nenne nämlich diesen Ausdruck Gz und setze $Gz = Fz + Rz$, wo Rz den Divisions-Rest bedeutet, den man erhält, wenn man Gz durch Fz dividirt. Setzt man nun statt z den Werth β^p und bedenkt, dafs $G\beta^p = 0$ ist, so erhält man $F\beta^p + R\beta^p = 0$.

Und da nun $F\beta^p \equiv 0 \pmod{p^m, \beta}$ ist, so mufs auch $R\beta^p \equiv 0 \pmod{p^m, \beta}$ sein, und folglich Rx die Form $p^m R_1 z$ haben (§. 56.), wo $R_1 z$ einen Ausdruck von z bedeutet. Man erhält daher $Gz = Fz + p^m R_1 z$ oder $Gz \equiv Fz \pmod{p^m}$.

Zusatz 2. Es ist in (§. 59.) gezeigt worden, dafs es $p^{(m-1)n}$ einfache Ausdrücke giebt, die mit fx nach dem Modul p congruent, die aber nach dem Modul p^m verschieden sind. Entwickelt man nun einen einfachen Ausdruck, dessen Wurzeln die $(p^{m-1})^{\text{ten}}$ Potenzen der Wurzeln irgend eines dieser Ausdrücke sind, so wird man nach dem Modul p^m stets denselben Ausdruck erhalten. Bezeichnet man nämlich wie oben einen solchen Ausdruck durch Fx, so erhält man $x^{p^n-1} - 1 = Fx\,Qx + p^m Rx$ (vergl. diesen §.), oder man hat $x^{p^n-1} - 1 \equiv Fx\,Qx \pmod{p^m}$ und weifs zugleich, dafs $Fx \equiv fx \pmod{p}$ ist. Da aber nun Fx und Qx keinen gemeinschaftlichen Theiler nach dem Modul p haben können (§. 45.), so kann es nicht noch ein Paar Factoren $F_1 x$ und $Q_1 x$ der Art geben, dafs $x^{p^n-1} - 1 \equiv F_1 x\,Q_1 x \pmod{p^m}$, und $F_1 x \equiv fx \pmod{p}$ sei (§. 59.). Dies müfste aber der Fall sein, wenn zwei Ausdrücke, die nach dem Modul p congruent, nach dem Modul p^m aber verschieden sind, nach dem Modul p^m zwei verschiedene Ausdrücke erzeugten, indem man diejenigen Ausdrücke entwickelte, die von ihren Wurzeln die $(p^m)^{\text{ten}}$ Potenzen enthielten.

Von den zusammengesetzten Moduln.

§. 65.

Ist der Modul von der Form $a^\alpha b^\beta c^\gamma$ etc., wo a, b, c etc. verschiedene Primzahlen und α, β, γ etc. natürlich ganze positive Exponenten bedeuten, so leitet man leicht folgenden Satz ab: Wenn mx und Mx Ausdrücke von x bedeuten, die nach den einzelnen Moduln a^α, b^β, c^γ etc. congruent sind, so sind diese beiden Ausdrücke auch nach dem Modul $a^\alpha b^\beta c^\gamma$ etc. congruent. Bezeichnet man nämlich zwei entsprechende Coëfficienten von Mx und mx durch A und a, so erhält man $A - a \equiv 0 \pmod{a^\alpha}$, $A - a \equiv 0 \pmod{b^\beta}$, $A - a \equiv 0 \pmod{c^\gamma}$ etc. und daher $A - a \equiv 0 \pmod{a^\alpha b^\beta c^\gamma}$ etc.) oder $A \equiv a \pmod{a^\alpha b^\beta c^\gamma}$ etc.). Da also alle entsprechenden Coëfficienten von Mx und mx nach dem Modul $a^\alpha b^\beta c^\gamma$ etc. übereinstimmen, so sind sie selbst nach diesem Modul congruent.

Zusatz. Aus dem vorherstehenden Satze ergiebt sich unmittelbar folgender: Läfst sich ein Ausdruck von x durch einen zweiten, in Bezug auf die einzelnen Moduln a^α, b^β, c^γ etc. ohne Rest theilen, so läfst er sich auch in Bezug auf den Modul $a^\alpha b^\beta c^\gamma$ etc. durch diesen Ausdruck ohne Rest theilen.

§. 66.

Lehrsatz. Ist Fx ein einfacher Ausdruck, so kann man die Zahlen z und z_1 stets so bestimmen, dafs $(x^z-1)^{z_1}$ durch Fx in Bezug auf den Modul $a^\alpha b^\beta c^\gamma$ etc. sich theilen lasse.

Beweis. Zunächst bemerke man, dafs, wenn ein Ausdruck fx in Bezug auf den Modul a^α irreductibel ist, so ist er entweder in Bezug auf a selbst irreductibel, oder die Potenz eines irreductibeln Ausdrucks (§. 60.). Für den ersten Fall folgt aus (§. 62.), dafs fx ein Divisor von $x^{a^{\alpha-1}(a^n-1)}-1$ sei, wo n den Grad von fx angiebt. Für den zweiten Fall setze man $n=n_1 z$, wo n_1 und z ganze Zahlen bedeuten, und $fx=\varphi x^{n_1}+p\psi x$, wo φx ein einfacher irreductibler Ausdruck vom Grade z in Bezug auf den Modul p ist: so ist φx in Bezug auf den Modul a ein Theiler von $x^{a^{z_1}-1}-1$ (§. 18.); woraus folgt, dafs $(x^{a^{z_1}-1}-1)^{n_1}$ in Bezug auf den Modul a den Factor φx^{n_1} habe, und dafs man ferner in Bezug auf denselben Modul auch fx oder $\varphi x^{n_1}+p\psi x$ als Factor von $(x^{a^{z_1}-1}-1)^{n_1}$ ansehen könne. Da nun $(x^{a^{z_1}-1}-1)^{n_1}$ in Bezug auf den Modul a den Factor fx in sich schliefst, so mufs $(x^{a^{z_1}-1}-1)^{n_1 a^{\alpha-1}}$ in Bezug auf den Modul a^α den Factor fx in sich schliefsen. Hieraus folgt nun zunächst, dafs man, wenn fx in Bezug auf den Modul a^α irreductibel ist, stets die Zahlen t und t_1 so bestimmen könne, dafs fx in Bezug auf den Modul a^α ein Factor von $(x^t-1)^{t_1}$ werde. Enthält nun Fx in Bezug auf den Modul a^α die einfachen irreductibeln Factoren fx, f_1x, f_2x etc., so bestimme man t_2 und t_3 so, dafs $(x^{t_2}-1)^{t_3}$ in Bezug auf den Modul a^α den Factor f_1x habe, und t_4 und t_5 so, dafs $(x^{t_4}-1)^{t_5}$ in Bezug auf denselben Modul den Factor f_2x habe etc. Nennt man dann T das kleinste gemeinschaftliche Vielfache von t, t_0, t_2 etc., und T_1 die Summe von $t_1+t_3+t_5+$ etc., so folgt leicht, dafs $(x^T-1)^{T_1}$ den Factor Fx in Bezug auf den Modul a^α in sich schliefsen werde. Bildet man nun noch die Ausdrücke $(x^S-1)^{S_1}$, $(x^V-1)^{V_1}$ etc., welche in Bezug auf die Moduln b^β, c^γ etc. Fx als Factor enthalten, so folgt zunächst, dafs $(x^T-1)^{T_1}(x^S-1)^{S_1}(x^V-1)^{V_1}\ldots.$ in Bezug auf den Modul $a^\alpha b^\beta c^\gamma$ etc. den Factor Fx enthalte (§. 65.). Es erhellet aber auch leicht, dafs, wenn z das kleinste gemeinschaftliche Vielfache von T, S, V etc., und z_1 die Summe von T_1, S_1, V_1 etc. ist, dafs alsdann $(x^z-1)^{z_1}$ in Bezug auf den Modul $a^\alpha b^\beta c^\gamma$ den Factor Fx in sich schliefsen werde. (§. 65.)

Brandenburg, den 3ten April 1846.