Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen.

Von **Richard Kantor** in Wien.

§ 1. Einleitung, einige allgemeine Sätze über die Wertigkeitsbestimmung mit Anwendungen.

Die vorliegende Abhandlung ist ein Auszug aus der Dissertation des Verfassers und beschäftigt sich mit folgendem Problem:

Wie viele nach irgend einem Modul m inkongruente Werte erhält eine ganze, rationale Funktion $f(x_1, x_2, \ldots x_n)$, wenn ihre (unabhängigen) Variabeln $x_1, x_2, \ldots x_n$ ein vollständiges Restsystem mod m durchlaufen? Die gesuchte Anzahl nennen wir die „Wertigkeit der Funktion $f(x_1, x_2, \ldots x_n)$". Die Wertigkeit kubischer Funktionen von einer Variabeln nach einem Primzahlmodul hat Daublebsky v. Sterneck (1907, Sitzungsberichte der kais. Akademie der Wissenschaften in Wien, Band CXVI, Abteilung II *a*) bestimmt; hier sollen zunächst einige allgemeine Sätze über die Wertigkeitsbestimmung Aufnahme finden, ferner die Wertigkeitsbestimmung kubischer Funktionen von einer Variabeln nach einem beliebigen Modul vollständig erledigt, endlich noch die Wertigkeitsbestimmung quadratischer Funktionen von beliebig vielen Variabeln kurz gestreift werden.

Unmittelbar ersichtlich sind folgende zwei Sätze:

I. Um die Wertigkeit $W(m)$ einer Funktion nach einem Modul m zu bestimmen, genügt es, ihre Wertigkeit nach jeder in diesem Modul aufgehenden Primzahlpotenz zu kennen, da wenn $m = p_1^{\alpha_1} p_2^{\alpha_2} p_\mu^{\alpha_\mu}$ ($p_i \neq p_k$, wenn $i \neq k$), die Formel gilt: (1) $W(m) = W(p_1^{\alpha_1}) W(p_2^{\alpha_2}) W(p_\mu^{\alpha_\mu})$.

II. Die Addition einer beliebigen Konstanten zu einer Funktion und ihre Multiplikation mit einer zum Modul m teilerfremden Konstanten haben auf die Wertigkeit der Funktion keinen Einfluß.

Die nächstfolgenden Sätze gelten für einen Primzahlmodul p und werden darin die Funktionen als nach dem Fermatschen Satz reduziert vorausgesetzt.

Die Konstanten sind einwertige Funktionen, umgekehrt

III. Die einzigen einwertigen Funktionen mod p sind die Konstanten.

Wir beweisen den Satz zunächst für eine Variable. A sei der einzige Wert, den die Funktion $f(x)$ annimmt; wir stellen uns die Aufgabe, die Koeffizienten von $f(x)$ zu bestimmen. Sei also $f(x) \equiv c_{p-1} x^{p-1} + c_{p-2} x^{p-2} + \cdots + c_1 x + c_0 \bmod p$. Für $x \equiv 0 \bmod p$ ergibt sich $c_0 \equiv A \bmod p$; setzt man sukzessive $x \equiv 1, 2, p-1 \bmod p$, so erhält man die $(p-1)$ Kongruenzen

$$\sum_{i=1}^{p-2} c_i x^i + c_{p-1} \equiv 0 \bmod p,\ x \equiv 1, 2, p-1 \bmod p, \qquad (1)$$

deren Addition ergibt $\sum_{i=1}^{p-2} c_i \left(\sum_{x \equiv 1}^{p-1} x^i \right) + (p-1) c_{p-1} \equiv 0 \bmod p$ und, da für $i \not\equiv 0 \bmod p-1$ $\sum_{x \equiv 1}^{p-1} x^i \equiv 0 \bmod p$, folgt $c_{p-1} \equiv 0 \bmod p$, wodurch die Kongruenzen (1) übergehen in

$$\sum_{i=1}^{p-2} c_i x^{i-1} \equiv 0 \bmod p;\ x \equiv 1, 2, p-1 \bmod p, \qquad (1a)$$

deren Addition $\sum_{i=2}^{p-2} c_i \left(\sum_{x \equiv 1}^{p-1} x^{i-1} \right) + (p-1) c_1 \equiv (p-1) c_1 \equiv 0 \bmod p$, $c_1 \equiv 0 \bmod p$ liefert. Auf dieselbe Art fortfahrend erhalten wir $c_1 \equiv c_2 \equiv c_{p-1} \equiv 0 \bmod p$, d. h. c_0 ist der einzige wirklich auftretende Koeffizient, $f(x)$ also eine Konstante.

Der Satz sei nun für n Variable bewiesen. Dann ordnen wir eine Funktion von $(n+1)$ Variabeln nach einer dieser Variabeln $f(x_1, \ldots x_{n+1}) \equiv c_{p-1} x_{n+1}^{p-1} + \cdots + c_0 \bmod p$, wo nun die c_i Funktionen von x_1, x_n sind. Soll $f(x_1, \ldots x_{n+1})$ einwertig sein, so ergibt sich, genau wie oben, daß sich $f(x_1, \ldots x_{n+1})$ auf c_0 reduziert. Dieses ist aber eine Funktion von n Variabeln, der Voraussetzung nach also eine Konstante, da c_0 einwertig sein soll, womit der Satz durch vollständige Induktion bewiesen ist.

Aus der Tatsache, daß eine Kongruenz n^{ten} Grades mod p höchstens n inkongruente Wurzeln hat, ergibt sich sofort der Satz:

IV. Lineare Funktionen mod p sind p-wertig; für die Wertigkeit k mod p einer Funktion n^{ten} Grades,

wo $2 \leqq n \leqq p-1$, gilt die Ungleichung $\left[\frac{p}{n}\right]+1 \leqq k \leqq p$ $\left(\left[\frac{p}{n}\right]$ höchste ganze Zahl $< \frac{p}{n}\right)$.

Ähnlich wie III beweist man:

V. Eine Funktion $(p-1)^{\text{ten}}$ Grades mod p kann nicht p-wertig sein.

VI. Man kann stets Funktionen mod p herstellen, welche an vorgeschriebenen Stellen vorgeschriebene Werte annehmen; sind für alle Stellen 0, 1, $p-1$ Funktionswerte vorgeschrieben, so ist die Funktion eindeutig bestimmt; daraus folgt unmittelbar, daß man Funktionen von jeder vorgeschriebenen Wertigkeit $k\,(1 \leqq k \leqq p)$ herstellen kann.

Sind nicht für alle Stellen Werte vorgeschrieben, so kann man die Werte an jenen Stellen, für welche keine Funktionswerte vorgeschrieben sind, willkürlich wählen und damit ist dieser Fall auf den zurückgeführt, daß für alle Stellen Funktionswerte vorgeschrieben sind. Es werde also gefordert, daß die gesuchte Funktion an der Stelle $x \equiv i \bmod p$ den Wert $f(i)$ annehme und unsere Aufgabe ist, die Koeffizienten $c_0\, c_1\, c_{p-1}$ der Funktion zu bestimmen. Es ist $c_0 \equiv f(0)$, im übrigen gelten die Kongruenzen

$$\sum_{i=1}^{p-2} c_i x^i + c_{p-1} \equiv f(x) - f(0) \bmod p,\ x \equiv 1, 2, p-1 \bmod p. \quad (2)$$

Sind diese Kongruenzen nach c_1, c_2, c_{p-1} auflösbar, so ist unser Satz bewiesen; sie sind tatsächlich auflösbar, da die Determinante der Koeffizienten der c:

$$D \equiv \begin{vmatrix} 1^{p-2} & 1^{p-3} & 1^1 & 1 \\ 2^{p-2} & 2^{p-3} & 2^1 & 1 \\ \cdots & \cdots & \cdots & \cdots \\ (p-1)^{p-2} & (p-1)^{p-3} & (p-1) & 1 \end{vmatrix} \not\equiv 0 \bmod p. \quad (3)$$

VII. Die Anzahl aller k-wertigen Funktionen mod p ist:

$$F_k = \binom{p}{k} \cdot \sum_{(\alpha)} \frac{p!}{\alpha_1!\, \alpha_2! \ldots \alpha_k!}, \quad (4)$$

wo die Summe zu erstrecken ist über alle Kombinationen $k$ter Klasse aus den Zahlklassen des vollständigen Restsystems mod p, die der Bedingung

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k = p \quad 0 < \alpha_i \leqq p \quad (5)$$

genügen.

Denn ein einzelner Posten unter dem Summenzeichen ist die Anzahl der verschiedenen Permutationen von p Elementen, unter welchen $\alpha_1, \alpha_2, \ldots \alpha_k$ gleiche Elemente vorkommen. Sind also A_1, A_2, A_k, k bestimmte Werte der Reihe $0, 1, p-1$, so zeigt ein einzelner Posten der obigen Summe an, auf wie viele Arten A_1, A_2, A_k als Funktionswerte auf die Argumentwerte in der Weise verteilt werden können, daß z. B. A_1 $\alpha_1 =$ mal, A_2 $\alpha_2 =$ mal, A_k $\alpha_k =$ mal angenommen wird, wo die α vorerst bestimmte Werte gemäß Bedingung (5) vorstellen; läßt man die α alle ihre Wertekombinationen durchlaufen, so erkennt man, daß die Summe in (4) die Anzahl aller Funktionen angibt, welche k bestimmte Funktionswerte A_1, A_2, A_k und nur diese annehmen. A_1, A_2, A_k ihrerseits können nun in $\binom{p}{k}$-facher Weise aus der Reihe $0, 1, p-1$ gewählt werden. Hieraus ergibt sich die Richtigkeit der Formel (4), von welcher wir noch folgende Spezialfälle angeben:

$$F_1 = p,\ F_p = p!,\ F_2 = p(p-1)(2^{p-1}-1)$$

$$F_{p-1} = p \cdot (p-1) \cdot \frac{p!}{2} \quad (p \neq 2) \quad (4a)$$

$\sum_{k=1}^{p} F_k$ bezw. $\sum_{k=2}^{p} F_k$, je nachdem die Konstanten mitgezählt werden oder nicht, ist die Anzahl aller nach dem Fermatschen Satz reduzierten Funktionen; zählt man diese statt nach ihrer Wertigkeit nach ihrem Grad ab, so erhält man die Formeln:

$$p^p = \sum_{k=1}^{p} \binom{p}{k} \sum_{(\alpha)} \frac{p!}{\alpha_1!\,\alpha_2! \ldots \alpha_k!} \quad (6)$$

und

$$\nu^p - p = \sum_{k=2}^{p} \binom{p}{k} \sum_{(\alpha)} \frac{p!}{\alpha_1!\,\alpha_2! \ldots \alpha_k!} \quad (6a)$$

mit der Summationsbedingung $\alpha_1 + \alpha_2 + \cdots + \alpha_k = p$; $0 < \alpha_i \leq p$.

Leicht zu beweisen sind die folgenden zwei Sätze:

VIII. Die Wertigkeit einer Funktion $f(x)$ mod m ändert sich nicht, wenn man an Stelle von x eine neue Variable ξ einführt, so daß $x \equiv \varphi(\xi) \bmod m$ eine m-wertige Funktion ist.

Dasselbe gilt für mehrere Variable, vorausgesetzt, daß die Funktionen

$$x_1 \equiv \varphi_1(\xi_1\, \xi_2\, \xi_n)\ x_2 \equiv \varphi_2(\xi_1\, \xi_2\, \xi_n) \ldots x_n \equiv \varphi_n(\xi_1\, \xi_2\, \xi_n) \bmod m$$

voneinander unabhängig sind.

IX. Ist $f(x)$ mod m eine m-wertige Funktion, so wird, wenn man an Stelle von x eine neue Variable ξ einführt, so daß $x \equiv \varphi(\xi)$ mod m eine k-wertige Funktion ist, auch $f[\varphi(\xi)]$ k-wertig.

Anwendungen auf Wertigkeitsbestimmungen nach einem Primzahlmodul p.

1. Die $k$ten Potenzen linearer Funktionen durchlaufen $\frac{p-1}{\delta}+1$ mod p inkongruente Werte, wo δ den größten, gemeinsamen Teiler von k und $p-1$ bedeutet.

2. Die Funktionen von der Gestalt

$$\left(\left(\left([a x^k + b_1]^{k_1} + b_2\right)^{k_2} + b_3\right)^{k_3} + \cdots\right),$$

wo $k, k_1, k_2 \ldots$ zu $(p-1)$ teilerfremd sind, sind p-wertig.

3. Ist $p \equiv 2$ mod 3, so sind alle p-wertigen Funktionen dritten Grades die dritten Potenzen linearer Funktionen, abgesehen von additiven und multiplikativen Konstanten. Mit Hilfe der Resultate Sternecks zu beweisen.

4. Die Funktion $a x^{2k} + b x^k$ durchläuft, wenn k zu $(p-1)$ relativ prim ist, $\frac{p+1}{2}$ mod p inkongruente Werte. Das ist nämlich die Wertigkeit einer beliebigen quadratischen Funktion mod p $(p \neq 2)$, wie man leicht beweist, indem man sie durch eine lineare Transformation auf die Form $a x^2$ bringt. Speziell $k = p-2$ $p \geqq 5$ $f(x) \equiv a x^{2(p-2)} + b x^{p-2} \equiv b x^{p-2} + a x^{p-3}$ mod p durchläuft $\frac{p+1}{2}$ inkongruente Werte.

5. Die Funktion $a x^{3k} + b x^{2k} + c x^k$, k zu $p-1$ relativ prim, durchläuft $\left\{\frac{2p}{3}\right\}$ inkongruente Werte, wenn $b^2 - 3ac \not\equiv 0$ mod p, p inkongruente Werte, wenn $b^2 - 3ac \equiv 0$ mod p und $p \equiv 2$ mod 3, $\frac{p+2}{3}$, wenn $b^2 - 3ac \equiv 0$ mod p und $p \equiv 1$ mod 3. Diese Resultate erhält nämlich Sterneck für $k = 1$. $\left\{\frac{2p}{3}\right\}$ ist die $\frac{2p}{3}$ zunächst liegende ganze Zahl $(p \neq 3)$. Speziell $k = p-2$ $f(x) \equiv a x^{3(p-2)} + b x^{2(p-2)} + c x^{p-2} \equiv c x^{p-2} + b x^{p-3} + a x^{p-4}$ mod p.

6. $(a x^2 + b x)^k$, k zu $p-1$ relativ prim, durchläuft $\frac{p+1}{2}$ inkongruente Werte.

7. $(a x^3 + b x^2 + c x)^k$, k zu $p-1$ relativ prim, durchläuft je nach den in 5 angegebenen Unterschieden $\left\{\frac{2p}{3}\right\}$, p, $\frac{p+2}{3}$ inkongruente Werte.

§ 2. Transformation kubischer Funktionen mod p^π in ihre für die Wertigkeitsbestimmung einfachste Form.

Wir führen in die allgemeinste kubische Funktion

$$f(x) \equiv a x^3 + b x^2 + c x + d \bmod p^\pi \tag{1}$$

die an der Wertigkeit nichts ändernde Substitution

$$x \equiv \xi + \lambda \bmod p^\pi \tag{2}$$

ein, durch welche (1) übergeht in

$$a \xi^3 + (3 a \lambda + b) \xi^2 + (3 a \lambda^2 + 2 b \lambda + c) \xi + \text{Konstante} \tag{1a}$$

und trachten λ so zu bestimmen, daß eines der Glieder von (1a) verschwindet. Die Bedingung für das Verschwinden des quadratischen Gliedes ist:

$$3 a \lambda + b \equiv 0 \bmod p^\pi, \tag{3}$$

die für das Verschwinden des linearen Gliedes

$$3 a \lambda^2 + 2 b \lambda + c \equiv 0 \bmod p^\pi. \tag{4}$$

Der Fall, daß $a \equiv 0 \bmod p$, $b \equiv 0 \bmod p$, $c \not\equiv 0 \bmod p$ führt bei jedem p leicht dazu, daß die Wertigkeit p^π ist. Wir schalten also diesen Fall aus und betrachten

I. $p \neq 3$, $a \not\equiv 0 \bmod p$. In diesem Fall ist die Kongruenz (3) lösbar, man kann also (1) in der Form

$$a' x^3 + c' x \equiv f(x) \bmod p^\pi \tag{1b}$$

voraussetzen, worin $a' \not\equiv 0 \bmod p$ und $c' \equiv 0 \bmod p^n \not\equiv 0 \bmod p^{n+1}$, wenn $b^2 - 3 a c \equiv 0 \bmod p^n \not\equiv 0 \bmod p^{n+1}$, $0 \leq n \leq \pi$. Dies wird bewiesen, indem man den Wert von λ aus (3) in

$$3 a \lambda^2 + 2 b \lambda + c \equiv 0 \bmod p^n \not\equiv 0 \bmod p^{n+1} \tag{4a}$$

einsetzt.

II. $p = 3$, $a \not\equiv 0 \bmod 3$ und 1. $b \not\equiv 0 \bmod 3$; (3) ist nicht lösbar, hingegen (4), so daß (1) in der Form

$$f(x) \equiv a' x^3 + b' x^2 \bmod 3^\pi, \; a', \; b' \not\equiv 0 \; (3) \tag{5}$$

vorausgesetzt werden kann.

2. $b \equiv 0 \bmod 3$; (3) ist lösbar, so daß (1) in der Form (1 b) vorausgesetzt werden kann, worin $c' \not\equiv 0 \bmod 3$, wenn $c \not\equiv 0 \bmod 3$ und $c' \equiv 0 \bmod 3^n \not\equiv 0 \bmod 3^{n+1}$, wenn $\beta^2 - a\gamma \equiv 0 \bmod 3^{n-1} \not\equiv 0 \bmod 3^n$, wobei $b \equiv 3\beta\,(3^\pi), c \equiv 3\gamma\,(3^\pi)$ gesetzt wurde. Zu beweisen wie I.

III. $p > 2, a \equiv 0 \bmod p, b \not\equiv 0 \bmod p$; (3) nicht erfüllbar, (4) erfüllbar; also kann (1) in der Form

$$f(x) \equiv a' x^3 + b' x^2 \bmod p^\pi,\ a' \equiv 0 \bmod p,\ b' \not\equiv 0 \bmod p \qquad (1\,c)$$

vorausgesetzt werden.

IV. $p = 2, a \equiv 0 \bmod 2, b \not\equiv 0 \bmod 2$; (3) nicht erfüllbar, (4) erfüllbar, wenn $a \equiv 0 \bmod 4$, $c \equiv 0 \bmod 2$ oder $a \equiv 0 \bmod 2 \not\equiv 0 \bmod 4$, $c \equiv 0 \bmod 4$; in diesen Fällen kann man also (1) in der Form (1 c) voraussetzen, während sonst auch (4) unerfüllbar ist, weshalb (1) in seiner ursprünglichen Form genommen werden muß.

In den folgenden Paragraphen werden wir zu jeder Methode der Wertigkeitsbestimmung ein einfaches Beispiel geben und zum Schlusse eine Tabelle der Wertigkeitsformeln für kubische Funktionen von einer Variabeln geben, wobei die Ableitung der betreffenden Formeln kurz angedeutet werden wird.

§ 3. Methoden der vollständigen Induktion und der einzelnen Potenzexponenten.

Um die Wertigkeit von $x^3 \bmod p^\pi$ zu bestimmen, überlegen wir uns leicht, daß für $x \equiv \lambda . p^\delta (p^\pi)$, $\delta > \left[\frac{\pi - 1}{3}\right]$ stets der Wert 0 erscheint, sonst aber die Kongruenz

$$\lambda^3 p^{3\delta} \equiv \lambda_1^3 p^{3\delta_1} \bmod p^\pi,\ \lambda,\ \lambda_1 \not\equiv 0 \bmod p \qquad (1)$$

nur bestehen kann, wenn $\delta = \delta_1$, in welchem Falle aus ihr

$$\lambda^3 \equiv \lambda_1^3 \bmod p^{\pi - 3\delta} \qquad (2)$$

folgt. Somit haben wir bloß die durch p unteilbaren kubischen Reste mod p^π abzuzählen und die betreffenden Formeln auch für die Moduln $p^{\pi - 3\delta}\left(\delta \leq \left[\frac{\pi - 1}{3}\right]\right)$ anzuwenden. Um dies zu bewerkstelligen, fragen wir danach, ob, wenn die Kongruenz

$$x^3 \equiv D \bmod p^{\pi - 1},\ D \not\equiv 0 \bmod p,\ p \neq 3 \qquad (3)$$

eine Lösung x_0 besitzt, auch jede der Kongruenzen

$$x^3 \equiv D + \mu . p^{\pi - 1} \bmod p^\pi,\ \mu = 0,\ 1,\ p - 1 \qquad (4)$$

eine Lösung besitzt; wegen der Voraussetzung der Lösbarkeit von (3) gibt es sicher μ-Werte, für welche Lösungen von (4) in der Gestalt

$$x_0 + \lambda . p^{\pi-1} \tag{5}$$

existieren; können wir tatsächlich die Existenz von Lösungen von (4) für jedes μ beweisen, so folgt, wenn $\overline{A}(p^\pi)$ die Wertigkeit von $x^3 \bmod p^\pi$ an den Stellen $x \not\equiv 0 \bmod p$ bezeichnet:

$$\overline{A}(p^\pi) = p\,\overline{A}(p^{\pi-1}) = \cdots = p^{\pi-1}\,\overline{A}(p) = p^{\pi-1} . \frac{p-1}{\delta}, \tag{6}$$

δ größter, gemeinsamer Teiler von 3 und $p-1$. Die Einsetzung von (5) in (4) ergibt aber die wegen $x_0 \not\equiv 0 \bmod p$ nach λ stets lösbare Kongruenz

$$3 x_0^2 \lambda \equiv \mu + \varkappa \bmod p, \tag{7}$$

wo $-x_0^3 + D = \varkappa . p^{\pi-1}$ gesetzt wurde, womit die Formel (6) bewiesen ist.

Etwas anders müssen wir bei $p = 3$ vorgehen. Hier folgt aus der Existenz einer Lösung x_0 der Kongruenz

$$x^3 \equiv D \bmod 3^\pi \tag{8}$$

die Existenz der drei Lösungen $x_0 + \lambda . 3^{\pi-1}$, $\lambda = 0, 1, 2$; setzt man hingegen in (8) für $x \mid x_0 + \lambda . 3^{\pi-2}$, so erhält man für $D \mid D + \mu . 3^{\pi-1}$; unsere Frage ist, ob man auf diese Art jedes $\mu = 0, 1, 2$ erhalten kann. Für $\pi \geq 3$ erhalten wir die Kongruenz

$$\lambda \equiv \mu + \varkappa \bmod 3, \tag{9}$$

aus welcher sich ergibt

$$\overline{A}(3^\pi) = 3 . \overline{A}(3^{\pi-1}) = 3^{\pi-2}\,\overline{A}(9) = 2 . 3^{\pi-2}, \tag{10}$$

wo $\overline{A}(3^\pi)$ die Wertigkeit von $x^3 \bmod 3^\pi$ an den Stellen $x \not\equiv 0$ (3) ist.

§ 4. Methode der konjugierten Werte.

Zwei Werte x, x_1 des vollständigen Restsystems mod p^π heißen „konjugiert bezüglich der Funktion $f(x)$“, wenn die Kongruenz

$$f(x) \equiv f(x_1) \bmod p^\pi \tag{1}$$

besteht. Wird in (1) x_1 als gegeben, x als Unbekannte betrachtet, so ist $x \equiv x_1 \bmod p^\pi$ selbstverständlich eine Lösung von (1), von

der wir aber absehen wollen; ergibt sich hingegen, daß die Kongruenz

$$\frac{f(x)-f(x_1)}{x-x_1} \equiv 0 \bmod p^\pi \qquad (1a)$$

ebenfalls die Lösung $x \equiv x_1 \bmod p^\pi$ besitzt, so nennen wir x_1 einen bezüglich der Funktion $f(x)$ „selbstkonjugierten" Wert. Ferner ist noch zu bemerken: Die Kongruenz

$$f(x).\varphi(x) \equiv 0 \bmod p^\pi \qquad (2)$$

kann gelöst werden:

1. Durch Werte ξ_1, für welche entweder $f(\xi_1)$ oder $\varphi(\xi_1) \equiv 0 \bmod p^\pi$,

2. durch Werte ξ_2, für welche $f(\xi_2) \equiv 0 \bmod p^\lambda$, $1 \leqq \lambda < \pi$, $f(\xi_2) \not\equiv 0 \bmod p^{\lambda+1}$ und gleichzeitig $\varphi(\xi_2) \equiv 0 \bmod p^{\pi-\lambda}$.

Die Lösungen der ersten Art sollen „totale Lösungen", die der zweiten Art „partielle Lösungen" heißen.

Wir können nun die Wertigkeit einer Funktion $f(x)$ bestimmen, indem wir nach der Anzahl der Lösungen von (1) fragen und wollen dieses Verfahren anwenden auf die Funktion

$$f(x) \equiv a x^3 + b x^2 \bmod p^\pi \; p > 2, \; a \equiv 0 \bmod p, \; b \not\equiv 0 \bmod p. \qquad (3)$$

Wir setzen also, wenn x_1 einen bestimmten Wert mod p^π bedeutet, an:

$$a x^3 + b x^2 \equiv a x_1^3 + b x_1^2 \bmod p^\pi \qquad (4)$$

oder

$$(x - x_1)\left[a x^2 + x\{a x_1 + b\} + a x_1^2 + b x_1\right] \equiv 0 \bmod p^\pi, \qquad (4a)$$

was nach Ausschaltung der Lösung $x \equiv x_1 \bmod p^\pi$ die wegen $a \equiv 0 \bmod p$, $a x_1 + b \not\equiv 0 \bmod p$ eindeutig lösbare Kongruenz für die totalen Lösungen von (4):

$$a x^2 + x(a x_1 + b) + a x_1^2 + b x_1 \equiv 0 \bmod p^\pi \qquad (5)$$

ergibt. Für die selbstkonjugierten x_1-Werte bekommt man die Kongruenz:

$$x_1(3 a x_1 + 2 b) \equiv 0 \bmod p^\pi \qquad (6)$$

mit der einzigen Lösung $x_1 \equiv 0 \bmod p^\pi$. Wir haben (4a) noch auf seine partiellen Lösungen zu untersuchen, $x = \bar{x}_1$ sei eine solche partielle Lösung: ist dies der Fall, so muß $x_1 \equiv \bar{x}_1 \bmod p^\lambda \not\equiv \bar{x}_1 \bmod p^{\lambda+1}$ und der zweite Faktor von (4a) muß mod $p^{\pi-\lambda}$ befriedigt werden, indem man für $x \mid \bar{x}_1$, für $x_1 \mid \bar{x}_1 + h.p^\lambda$ einsetzt. Subtrahiert man sodann den zweiten Faktor von (4a) von (6), so erhält man $\bar{x}_1 \equiv 0 \bmod p$.

Die Wertigkeit von (3) an den Stellen $x \not\equiv 0 \bmod p$ ist also gleich der Hälfte der Anzahl dieser Stellen, d. i. $\frac{p^\pi - p^{\pi-1}}{2}$. Setzen wir $x \equiv h \cdot p^\lambda \bmod p^\pi$, so ergibt sich für $\lambda > \left[\frac{\pi-1}{2}\right]$ 0, für $\lambda \leqq \left[\frac{\pi-1}{2}\right]$ ist die Wertigkeit von (2) an den Stellen $x \equiv h \cdot p^\lambda \bmod p^\pi, h \not\equiv 0 \bmod p$, identisch mit der Wertigkeit der Funktion

$$\varphi(h) \equiv a h^3 p^\lambda + b \cdot h^2 \bmod p^{\pi - 2\lambda} \tag{7}$$

an den Stellen $h \not\equiv 0 \bmod p$, welche Wertigkeitsbestimmung oben durchgeführt wurde.

§ 5. Methode des vollständigen Restsystems mod p.

Es kann vorkommen, daß, damit $f(x) \equiv f(x_1) \bmod p^\pi$ notwendig $x \equiv x_1 \bmod p$ sein muß. Dann ist es manchmal angezeigt, die Wertigkeit von $f(x)$ zu bestimmen, indem man sukzessive $x \equiv p \cdot \xi + \lambda \bmod p^\pi, \lambda = 0, 1, p-1$ setzt. Ersichtlich ist diese Methode nur brauchbar, wenn p eine kleine Zahl ist. Als Beispiel diene:

$$f(x) \equiv 2 a x^3 + b x^2 \bmod 2^\pi; a, b \not\equiv 0 \bmod 2. \tag{1}$$

Daraus, daß die Kongruenz

$$(x - x_1)\left[2a\{x^2 + x x_1 + x_1^2\} + b\{x + x_1\}\right] \equiv 0 \bmod 2^\pi$$

nur durch $x \equiv x_1 \bmod 2$ gelöst werden kann, folgt die Anwendbarkeit der Methode.

Setzt man also in (1) $x \equiv 2\xi \bmod 2^\pi$, so geht (1) über in die Funktion

$$\varphi_1(\xi) \equiv 4 a \xi^3 + b \xi^2 \bmod 2^{\pi-2}, \tag{2}$$

deren Wertigkeit nach der Methode der konjugierten Werte zu bestimmen ist.

Setzt man $x \equiv 2\xi + 1 \bmod 2^\pi$, so geht (1) zunächst in

$$\varphi_2(\xi) \equiv 4 a \xi^3 + \xi^2(6a + b) + \xi(3a + b) \bmod 2^{\pi-2}$$

und nach der Substitution $\xi \equiv y + \beta \bmod 2^{\pi-2}$, in welcher β so bestimmt wird, daß das lineare Glied verschwindet, was wegen $4a \equiv 0 \bmod 2$, $6a + b \not\equiv 0$ (2) möglich ist, in eine Funktion vom Typus (2) über.

§ 6. Tabellarische Übersicht der Wertigkeitsformeln für kubische Funktionen $f(x) \equiv ax^3 + bx^2 + cx + d \bmod p^\pi$.

Zeichenerklärung: $[n]$ = höchste ganze Zahl $\leqq n$; $\{n\}$ = die n zunächst liegende ganze Zahl; bei $p = 3$, $b \equiv 0 \bmod 3$, $c \equiv 0 \bmod 3$ wurde $b \equiv 3\beta \bmod 3^\pi$, $c = 3\gamma \bmod 3^\pi$ gesetzt; δ = größter gemeinsamer Teiler von 3 und $p-1$.

A. $p > 3$.

Nr.	Teilbarkeit durch p von				Weitere Bedingungen	Wertigkeitsformel
	a	b	c	$b^2 - 3ac$		
1	$\not\equiv 0\,(p)$			$\equiv 0\,(p^\pi)$		$\dfrac{p^{\pi+2} - p^{\pi - 3\cdot\left[\frac{\pi-1}{3}\right]-1}}{\delta(p^2+p+1)} + 1$
2	„			$\not\equiv 0\,(p)$		$p^{\pi-1} \cdot \left\{\dfrac{2p}{3}\right\}$
3	$\equiv 0\,(p)$	$\not\equiv 0\,(p)$				$\dfrac{p^{\pi+1} - p^{\pi-2\left[\frac{\pi-1}{2}\right]-1}}{2(p+1)} + 1$
4	„	$\equiv 0\,(p)$	$\not\equiv 0\,(p)$			p^π
5	$\not\equiv 0\,(p)$			$\equiv 0 (p^n) 0 < n < \pi$	$\pi - n - 1 < \dfrac{n}{2}$	wie unter 1
6	„			„	$\pi - n - 1 \geqq \dfrac{n}{2}\; n \equiv 0\,(2)$	$\dfrac{p^{\pi+2} - p^{\pi - \frac{3n}{2}+2}}{\delta(p^2+p+1)} + p^{\pi - \frac{3n+2}{2}} \cdot \left\{\dfrac{2p}{3}\right\}$
7	„			„	„ $n \not\equiv 0\,(2)$	$\dfrac{p^{\pi+2} - p^{\pi - \frac{3n-1}{2}}}{\delta(p^2+p+1)} + p^{\pi - \frac{3n+1}{2}}$

Bemerkungen zum Beweis der vorstehenden Formeln: ad 1. Vollständige Induktion und einzelne Exponenten. ad 2. Vollständige Induktion; das Nichtbestehen der Kongruenz (1) $3ax^2 + c' \equiv 0 \bmod p$ ist die Bedingung dafür, daß aus dem zu $x \bmod p^{\pi-1}$ gehörigen Funktionswert $D \bmod p^{\pi}$ sämtliche $D + \mu . p^{\pi-1} (\mu = 0, 1, \ldots p-1)$ entstehen; hiebei bedeutet $ax^3 + c'x$ die transformierte Form von $f(x)$; zu beweisen ist noch, daß alle Funktionswerte, die an Stellen auftreten, welche der Kongruenz (1) genügen, auch an Stellen auftreten, welche der Kongruenz (1) nicht genügen; dies folgt für $\pi = 1$ aus einem Satze über die elementarsymmetrischen Funktionen, für $\pi > 1$ durch vollständige Induktion. ad 3 und 4. Methode der konjugierten Werte. ad 5. Einzelne Exponenten; man konstatiert leicht, daß die Wertigkeit an den Stellen $x \equiv \lambda p^{\alpha} \bmod p^{\pi}$, $\alpha = 0, 1 \ldots \pi - n - 1$, $\lambda \not\equiv 0 \bmod p$, übereinstimmt mit der Wertigkeit von $f(y) \equiv a\lambda^3 \bmod p^{\pi-3\alpha}$ für $\lambda \not\equiv 0 \bmod p$, während für $\alpha > \pi - n - 1$ stets der Wert 0 auftritt. ad 6. Für $x \equiv \lambda p^{\alpha} (p^{\pi}), \lambda \not\equiv 0 (p), \alpha < \frac{n}{2}$ wie 5; dann betrachtet man die Werte $x \equiv \lambda p^{\frac{n}{2}} (p^{\pi})$, wo λ auch durch p teilbar sein kann und findet Übereinstimmung mit der Wertigkeit von

$$f(\lambda) \equiv a'\lambda^3 + c'\lambda \bmod p^{\pi - \frac{3n}{2}},\ a',\ c' \not\equiv 0 (p).$$

ad 7. Für $x \equiv \lambda p^{\alpha} (p^{\pi}), \lambda \not\equiv 0 (p), \alpha \leqq \frac{n-1}{2}$ wie 5; dann konstatiert man für die Werte $x \equiv \lambda p^{\alpha} (p^{\pi}), \frac{n+1}{2} \leqq \alpha \leqq \pi - n - 1$, Übereinstimmung mit der Wertigkeit der Funktion $f(\lambda) \equiv a'\lambda^3 p^{2\alpha-n} + c'\lambda \bmod p^{\pi-n-\alpha}$ für $\lambda \not\equiv 0 (p)$, welche Wertigkeit aus 4 leicht zu berechnen ist; für $\alpha > \pi - n - 1$ tritt nur der Wert 0 auf.

B. $p = 3$.

Nr.	Teilbarkeit durch 3 von a	b	c	$\beta^2 - a\gamma$	Weitere Bedingungen	Wertigkeitsformel	Bemerkungen zur Ableitung der betreffenden Formel
1	$\not\equiv 0\,(3)$	$\not\equiv 0\,(3)$				$2.3^{\pi-1}$	analog 2 in *A.*
2	„	$\equiv 0\,(3)$	$\not\equiv 0\,(3)$		$a + c \not\equiv 0\,(3)$	3^{π}	
3	„	„	„		$a + c \equiv 0\,(3)$	$3^{\pi-1}$	
4	„	„	$\equiv 0\,(3)$	$\equiv 0 \bmod 3^{\pi-1}$	$\pi - 1 \not\equiv 0 \bmod 3$	$1 + \frac{3^{\pi+1} - 3^{\pi-2-3\left\lfloor\frac{\pi-1}{3}\right\rfloor}}{13}$	analog 1 in *A.*
5	„	„	„	„	$\pi - 1 \equiv 0 \bmod 3$	$3 + \frac{3^{\pi+1} - 9}{13}$	
6	„	„	„	$\not\equiv 0 \bmod 3$	$a(\beta^2 - a\gamma) \equiv 1\,(3), \pi > 1$	$3^{\pi-1}$	vollständiges Restsystem mod 3
7	„	„	„	„	„ $\pi = 1$	3	
8	„	„	„	„	$a(\beta^2 - a\gamma) \equiv -1\,(3), \pi \geqq 4$	$13.3^{\pi-4}$	
9	„	„	„	„	„ $\pi = 3$	5	
10	„	„	„	„	„ $\pi = 1$ oder 2	3	
11	$\equiv 0\,(3)$	$\not\equiv 0\,(3)$				$\frac{3^{\pi+1} - 3^{\pi-2\left\lfloor\frac{\pi-1}{2}\right\rfloor}-1}{8} + 1$	konjugierte Werte

					3^π	konj. Werte
12	$\equiv 0(3)$	$\equiv 0(3)$	$\not\equiv 0(3)$			
13	$\not\equiv 0(3)$	"	$\equiv 0(3)$	$\equiv b'.3^{n-1}(3^\pi)$ $b' \not\equiv 0(3)$ $1 < n < \pi$	wie unter 4	analog 5 in A.
14	"	"	"	wie unter 13	" " 5	
15	"	"	"	"	$\frac{3^{\pi+1} - 3^{\pi+1-\frac{3n}{2}}}{13} + 3^{\pi-\frac{3n}{2}}$	analog 6 in A.
16	"	"	"	"	$\frac{3^{\pi+1} - 3^{\pi+1-\frac{3n}{2}}}{13} + 3^{\pi-\frac{3n}{2}-1}$	
17	"	"	"	"	$\frac{3^{\pi+1} - 3^{\pi+1-\frac{3(n-1)}{2}}}{13} + 3^{\pi-\frac{3(n-1)}{2}-1}$	analog 6 in A., indem man zuerst die Wertigkeit für $x \equiv \lambda \cdot 3^\alpha (3^\pi), \lambda \not\equiv 0 (3)$, $\alpha < \frac{n-1}{2}$, sodann für $x \equiv \lambda . 3^{\frac{n-1}{2}} (3^\pi)$, wobei λ auch $\equiv 0 (3)$ sein kann, bestimmt; die letzteren Werte führen auf die Wertigkeitsbestimmungen bezw 6—10 zurück.
18	"	"	"	"	$\frac{3^{\pi+1} - 9}{13} + 3$	
19	"	"	"	"	$\frac{3^{\pi+1} - 3^{\pi+1-\frac{3(n-1)}{2}}}{13} + 13 . 3^{\pi-\frac{3(n-1)}{2}-4}$	
20	"	"	"	"	$\frac{3^{\pi+1} - 81}{13} + 5$	
21	"	"	"	"	$\frac{3^{\pi+1} - 9 \text{ (oder } 27)}{13} + 3$	

C. $p = 2$.

Mit Ausnahme des Falles $a \equiv 0 \bmod 2$, $b \not\equiv 0 \bmod 2$ alle Formeln wie in *A.*; im genannten Ausnahmefall gelten folgende vier Formeln, von denen die ersten zwei nach der Methode der konjugierten Werte, die letzten zwei nach der Methode des vollständigen Restsystems mod 2 abgeleitet werden.

$$c \not\equiv 0\,(2) : 2^{\pi-1} \text{ für } \pi > 1 \text{ und } 2 \text{ für } \pi = 1 \tag{1}$$

$$a \equiv 0\,(4)\; c \equiv 0\,(2);\; 2 + 2^{\pi-2}\left[\frac{\pi-3}{2}\right] - 3\,\frac{4^{\left[\frac{\pi-3}{2}\right]+1} - 1}{3}$$
$$\text{für } \pi \geqq 3 \text{ und } 2 \text{ für } \pi = 1, 2 \tag{2}$$

$$a \equiv 0\,(2) \not\equiv 0\,(4)\; c \equiv 0\,(4) : 4 + 2^{\pi-2}\left[\frac{\pi-5}{2}\right] - 4 \cdot \frac{4^{\left[\frac{\pi-5}{2}\right]+1} - 1}{3}$$
$$\text{für } \pi \geqq 5;\; 4 \text{ für } \pi = 3, 4;\; 2 \text{ für } \pi = 1, 2 \tag{3}$$

$$a \equiv 0\,(2) \not\equiv 0\,(4)\;\; c \equiv 0\,(2) \not\equiv 0\,(4) : 2^{\pi-2} \text{ für } \pi > 2$$
$$\text{und } 2 \text{ für } \pi = 1, 2. \tag{4}$$

§ 7. Wertigkeitsbestimmung quadratischer Funktionen von beliebig vielen Variabeln nach einem Primzahlmodul $p \neq 2$.

I. Jede quadratische Funktion, welche nicht bis auf multiplikative und additive Konstante mit dem Quadrat einer linearen Funktion identisch ist, ist p-wertig; im genannten Ausnahmefall ist sie $\frac{p+1}{2}$-wertig.

Man betrachtet zunächst den Fall von 2 Variabeln x, y, also

$$f(x,y) \equiv a x^2 + b x y + c y^2 + d x + e y + f \bmod p. \tag{1}$$

Ist $a \not\equiv 0 \bmod p$, $c \not\equiv 0 \bmod p$, $b, d, e \equiv 0 \bmod p$, so ergibt sich obiger Satz aus der Tatsache, daß $a x^2 + c y^2 = D \bmod p$, $a, c \not\equiv 0\,(p)$ stets lösbar ist. Alle anderen Fälle lassen sich aber durch lineare Substitutionen auf den Fall $b, d, e \equiv 0 \bmod p$ zurückführen, wenn nicht $b^2 - 4ac \equiv 0 \bmod p$ und $2ae - bd \equiv 0 \bmod p$ (oder, was dasselbe ist, $2cd - be \equiv 0 \bmod p$). Sind aber beide letzteren Kongruenzen erfüllt, so ergibt eine einfache Umformung von (1): $4a e^2 f(x,y) \equiv (2aex + 2cdy + ed)^2 - e^2 d^2 + f \bmod p$. Für n Variable wird der Satz durch vollständige Induktion bewiesen. Eine einfache Verallgemeinerung des Satzes I ist:

II. Jede Funktion $f(x_1, x_2, \ldots x_n)$, in welcher eine oder mehrere Variable $x_1, x_2, \ldots x_m$ höchstens quadratisch vorkommen, jedoch nicht so, daß $f(x_1, x_2, \ldots x_n)$ für jedes Wertesystem der Variabeln $x_{m+1}, x_{m+2}, \ldots x_n$ in das Quadrat einer linearen Funktion, abgesehen von multiplikativen und additiven Konstanten übergeht, ist mod p. p-wertig.

Denn die Funktion $f(x_i, a_k)$ $(i = 1, 2, \ldots m)$, in welcher a_k bestimmte Werte für x_k $k = m + 1, \ldots n)$ bedeuten, ist p-wertig, wenn nicht $f(x_i\, a_k)$ abgesehen von Konstanten das Quadrat einer linearen Funktion ist, also ist schon ein Bestandteil von $f(x_1, x_2, \ldots x_n)$, umsomehr dieses selbst p-wertig.