ARKIV FÖR MATEMATIK Band 1 nr 21

Vorgelegt am 12. April 1950

Ein Problem bei dyadischer Zahlendarstellung

Von A. WIMAN

1. Bei gewissen Untersuchungen von p-Gruppen von maximaler Klasse stösst man auf eine Aufgabe, welche, freilich in umschriebener Gestalt, wir als Gegenstand für die folgende Note gewählt haben. Wir betrachten den Ausdruck $(1+x)^p$, wo p eine beliebige ganze Zahl >0 sein kann; das eigentliche Interesse knüpft sich jedoch an den Fall, wo p eine Primzahl bedeutet. Für diesen Ausdruck haben wir die Entwicklung:

$$(1)\qquad (1+x)^p = (1+x) + x(1+x) + x[1+x+x(1+x)] + x[\ ] + \cdots,$$

wo jeder folgende Klammer die ganze vorangehende Entwicklung enthält. In dieser Weise bekommen wir die vollständige Entwicklung nach p Klammern. Gehen wir für $p=5$ zur Potenzreihenentwicklung über, so ergibt sich aus (1):

$$\begin{aligned}(2)\qquad (1+x)^5 = {} & 1 + x + x + x^2 + x + x^2 + x^2 + x^3 + x + x^2 + x^2 + \\ & + x^3 + x^2 + x^3 + x^3 + x^4 + x + x^2 + x^2 + x^3 + x^2 + \\ & + x^3 + x^3 + x^4 + x^2 + x^3 + x^3 + x^4 + x^3 + x^4 + x^4 + x^5.\end{aligned}$$

Wie unmittelbar ersichtlich ist, bekommt man für jede folgende Potenz die Entwicklung aus derjenigen der vorangehenden, indem man letztere mit x multipliziert und hinzufügt. Wir denken uns jetzt für jeden Exponenten p eine Entwicklung von der Art (2). Die Frage, um welche es sich in den folgenden Auseinandersetzungen handelt, lässt sich so formulieren. Wir betrachten zwei beliebige Potenzen x^h und x^k mit $0<h<k<p$. Man soll berechnen, wie oft eine Potenz x^k früher als eine Potenz x^h in der Entwicklung auftritt. *Das eigentliche Ziel ist hier zu entscheiden, ob die gesuchte Anzahl durch p teilbar ist oder nicht.* Für h und k lässt sich noch die Beschränkung

$$(3)\qquad 0<h<k;\quad h+k\leqq p$$

einführen. Man sieht ja leicht, dass für h, k und $p-k$, $p-h$ dieselbe Antwort gilt.

Man sieht leicht ein, dass das obige Problem in nahem Zusammenhange mit der dyadischen Darstellung der ganzen Zahlen steht. Dies gelingt, indem man in (1) und (2) von den Potenzen zu den Exponenten übergeht. In (1) fangen wir mit $1+x$ an. Als zugehörige Exponenten hat man die einzifferigen dyadischen Zahlen 0 und 1. Im nächsten Abschnitte werden diese Exponenten um

1 erhöht; wir bezeichnen dieselben mit 10 und 11, also mit den zweizifferigen dyadischen Zahlen. Beim nächsten Abschnitte $x[1 + x + x(1 + x)]$ führen wir auch für die Exponenten von $1 + x$ zweizifferige Zahlen ein, nämlich 00 und 01. Für die vier Glieder im diesen Abschnitte bekommen wir also als Bezeichnungen der Exponenten die dreigliedrigen Zahlen 100, 101, 110 und 111. Wenn wir jetzt in (2) die Glieder mit den in solcher Weise bezeichneten Exponenten ersetzen, so bekommen wir die Folge:

(4) 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111, 10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111.

Wie man sieht, erhalten wir beim Übergang zu den Exponenten die dyadischen Zahlen nach steigender Grösse. Man beachte noch, dass einer Potenz x^h in (2) eine dyadische Zahl mit h Einsen in (4) entspricht. Für die Aufgabe, die wir zu lösen haben, ist also eine zweite Formulierung zulässig, nach welcher es zu entscheiden gilt, *wie oft unter den 2^p ersten dyadischen Zahlen eine Zahl mit k Einsen einer Zahl mit h Einsen vorangeht.* Für $p = 5$ sind nur vier Fälle zu untersuchen, nämlich: $h = 1$, $k = 2$; $h = 1$, $k = 3$; $h = 1$, $k = 4$; $h = 2$, $k = 3$. Die Antworten lassen sich hier leicht aus (2) oder (4) ablesen. Für die gesuchten Anzahlen führen wir die Bezeichnung $(k, h)_p$ ein und bekommen:

(5) $$(2, 1)_5 = 10;\ (3, 1)_5 = 5;\ (4, 1)_5 = 1;\ (3, 2)_5 = 24.$$

In den beiden ersten Fällen gibt mithin die Antwort durch $p = 5$ teilbare Zahlen, in den beiden letzteren aber nicht. Die Vermutung liegt jetzt nahe, dass dieser Unterschied darauf beruht, ob in (3) für $h + k$ das obere oder untere Zeichen gilt. *Ein Beweis für diese Vermutung wird in den folgenden Entwicklungen gegeben.*

2. Am einfachsten gelingt dies für die Fälle $h = 1$ und $h = 2$, welche wir in dieser Nummer behandeln werden. Wie (2) und (4) sich fortsetzen lassen, so dass dieselben gelten, wenn 5 durch eine höhere Zahl p ersetzt wird, versteht man unmittelbar. Eine so erweiterte Folge (4) lässt sich in p Abschnitte je nach der Zifferanzahl zerlegen. Wie viele Zahlen mit k Einsen gibt es nun in den n ersten Abschnitten? Offenbar ist die gesuchte Anzahl gleich dem Koeffizienten von x^k in der Entwicklung von $(1 + x)^n$, also:

(6) $$\frac{n(n-1)\cdots(n-k+1)}{\underline{|k}}.$$

Wir suchen noch die Anzahl der Zahlen mit h Einsen im $(n + 1)^{\text{ten}}$ Abschnitt. Die Antwort hier findet man in dem Koeffizienten für x^{h-1} in der Entwicklung von $(1 + x)^n$, also:

(7) $$\frac{n(n-1)\cdots(n-h+2)}{\underline{|h-1}}.$$

Für $h = 1$ gibt es selbstverständlich nur eine solche Zahl, und für die gesamte Anzahl von Kombinationen, in denen eine Zahl mit k Einsen einer Zahl mit h Einsen für $h = 1$ vorangeht, findet man:

$$\sum_{n=k}^{n=p-1} \frac{n(n-1)\cdots(n-k+1)}{\underline{|k}}. \tag{8}$$

Summiert man (8), so ergibt sich bekanntlich:

$$\frac{p(p-1)\cdots(p-k)}{\underline{|k}(k+1)}. \tag{9}$$

In (9) haben wir eine Zahl, welche offensichtlich, wenn p eine Primzahl ist, für $k+1<p$ durch p teilbar ist. Für $k+1=p$, ist dagegen diese Zahl $= 1$. Für $h = 1$ ist somit der Beweis gelungen.

Der Ausdruck (7) hat für $h = 2$ den Wert n. Wir suchen zuerst die Anzahl der Kombinationen, wo die Zahl mit k Einsen und diejenige mit h Einsen zu verschiedenen Abschnitten gehören, also von derselben Art wie für $h = 1$. Die Antwort erhält man durch Summieren der Produkte von (6) und (7). Als Resultat ergibt sich mithin für $h = 2$:

$$\sum_{n=k}^{n=p-1} \frac{n(n-1)\cdots(n-k+1)}{\underline{|k}} \cdot n. \tag{10}$$

Hierzu kommen noch die Kombinationen, wo die beiden Zahlen in demselben Abschnitt liegen. Wir nehmen an, der Abschnitt sei derjenige der $(n+1)$-zifferigen Zahlen. Da der erste Ziffer 1 ist, so können wir diesen weglassen. Was übrig bleibt, ist der Inbegriff der Zahlen, deren Zifferanzahl höchstens gleich n ist. Es müssen jetzt k und $h = 2$ um 1 vermindert, also durch $k-1$ und 1 ersetzt werden. Die Antwort hat man somit in (9), wenn man n für p und $k-1$ für k einführt. Zu (10) kommt mithin noch die Summe:

$$\sum_{n=k}^{n=p-1} \frac{n(n-1)\cdots(n-k+1)}{\underline{|k}}. \tag{11}$$

Es lassen sich (10) und (11) zusammenschlagen, indem man entsprechende Glieder addiert. Man erhält in solcher Weise:

$$\sum_{n=k}^{n=p-1} \frac{(n+1)n(n-1)\cdots(n-k+1)}{\underline{|k}}. \tag{12}$$

Als Wert dieser Summe ergibt sich:

$$\frac{(p+1)p(p-1)\cdots(p-k)}{\underline{|k}(k+2)}. \tag{13}$$

Ist p eine Primzahl, so hat (13) p als Teiler oder nicht, je nachdem $k+2<p$ oder $= p$ ist. Es war eben dies, was wir beweisen wollten.

3. Wir gehen jetzt zur Behandlung des allgemeinen Falles über. Für h und k gilt also nur die Beschränkung (3). Wie für den speziellen Fall $h = 2$ zerfällt die gesuchte Anzahl in zwei Teilsummen. Ist erstens die Zifferanzahl für die Zahl mit k Einsen nicht so gross wie für die Zahl mit h Einsen, so erhält man die entsprechende Teilsumme, indem man zuerst die Ausdrücke (6) und (7) mit einander multipliziert und dann nach n summiert, also in der Gestalt:

$$(14) \qquad \sum_{n=k}^{n=p-1} \frac{n(n-1)\cdots(n-k+1)}{\underline{|k}} \cdot \frac{n(n-1)\cdots(n-h+2)}{\underline{|h-1}}.$$

Die Summanden in (14) sind vom Grade $k + h - 1$ in n. Führt man die Summation aus, so ergibt sich also ein Resultat vom Grade $k + h$ in p. Für die Teilsumme, welche man erhält, wenn die beiden Zahlen mit k bzw. h Einsen von gleicher Zifferanzahl sind, lässt sich ein Ausdruck nicht so unmittelbar angeben. Nach einer in unserer ersten Nummer eingeführten Bezeichnung können wir für diese Summe schreiben:

$$(15) \qquad \sum_{n=k}^{n=p-1} (k-1, h-1)_n.$$

Wünscht man nun die Glieder von (15) näher zu bestimmen, so ist man offenbar auf ähnliche Summen wie (14) und (15), nur mit niedrigeren k- und h-Werten, zurückgewiesen. Geht man weiter fort in derselben Richtung, so endet man mit $(k - h + 1, 1)_p$, und von diesem Ausdruck lässt sich der Wert durch (9) bestimmen, wobei zu berücksichtigen ist, dass man k durch $k - h + 1$ ersetzt; der Grad in p ist also $k - h + 2$. Wir gehen jetzt den umgekehrten Weg, steigen also von $(k-i, h-i)_p$ zu $(k-i+1, h-i+1)_p$ für $i = h-1, h-2, \ldots 2$. Dies wird in zwei Schritten getan, indem zuerst eine Summe der Art (15) eingeführt wird, der man dann eine Summe der Art (14) hinzufügt. Bei jedem von diesen Schritten wird der Grad um eine Einheit erhöht. Es sind $2(h-2)$ Schritte erforderlich, um von $(k - h + 1, 1)_p$ zu $(k - 1, h - 1)_p$ hinaufzusteigen. Die Glieder in (15) sind mithin vom Grade $k - h + 2 + 2(h-2) = k + h - 2$ und ihre Summe vom Grade $k + h - 1$ in p. *Das Glied vom Grade $k + h$ in $(k, h)_p$ rührt also ausschliesslich von* (14) *her.* Die Summationen der Art (15), von denen hier die Rede ist, führen gewisse Zahlenfaktoren für den Nenner mit sich, doch keinen, der grösser als der erhaltene Grad in p ist. Es folgt hieraus, dass der Nenner von $(k-1, h-1)_n$ sich in Faktoren zerlegen lässt, von denen keiner grösser als $k + h - 2$ ist. Zuletzt ist hervorzuheben, dass auch die Glieder in (15) den Faktor $n(n-1)\cdots(n-k+1)$ enthalten müssen. Man versteht ja schon aus ihrer Bedeutung, dass die zugehörigen Ausdrücke in n für $n = 0, 1, \ldots, k-1$ gleich Null sein müssen. Übrigens sieht man aus den nächstfolgenden Entwicklungen, wie bei dem Übergange zu $(k, h)_n$ ein neuer Faktor $(n - k)$ hinzukommt.

4. Um $(k, h)_p$ zu berechnen, führen wir entsprechende Glieder von (14) und (15) zusammen und schreiben als Resultat:

$$(16) \qquad (k, h)_p = \sum_{n=k}^{n=p-1} \frac{n(n-1)\cdots(n-k+1)}{\underline{|k}} \varphi_{h-1}(n).$$

Dabei rührt das Glied von der Gradzahl $h-1$ in $\varphi_{h-1}(n)$ ausschliesslich von (14) her. Es ist hier vorteilhaft $\varphi_{h-1}(n)$ in eine Reihe zu entwickeln:

$$\varphi_{h-1}(n) = a_0 + a_1(n+1) + \cdots a_{h-1}(n+1)(n+2)\cdots(n+h-1). \tag{17}$$

Es geht dann (16) in eine Doppelreihe über, und man erhält:

$$(k,h)_p = \sum_{i=0}^{i=h-1} \sum_{n=k}^{n=p-1} \frac{a_i(n+i)(n+i-1)\cdots(n-k+1)}{\underline{|k}}. \tag{18}$$

Die erste Summation in (18) lässt sich unmittelbar ausführen, und es ergibt sich:

$$(k,h)_p = \sum_{i=0}^{i=h-1} \frac{a_i(p+i)\cdots p\cdots(p-k)}{\underline{|k}\cdot(k+i+1)}. \tag{19}$$

Von den Grössen a_i bestimmt man zuerst a_{h-1}, dann a_{h-2} und zuletzt a_0. Wie unmittelbar ersichtlich ist, hat man:

$$a_{h-1} = \frac{1}{\underline{|h-1}}.$$

In (19) nehmen wir nun zuerst das Glied

$$\frac{(p+h-1)(p+h-2)\cdots p\cdots(p-k)}{\underline{|k}\cdot\underline{|h-1}\cdot(k+h)} \tag{20}$$

in Betracht. Diese Zahl ist, wie man leicht sieht, eine ganze Zahl. Wir nehmen jetzt an, p sei eine Primzahl. Für $k+h<p$ muss dann (20) durch p teilbar sein. Hat man aber $k+h=p$, so enthält dagegen (20) den Faktor p nicht. In diesem Falle gilt für (20) die Kongruenz

$$\equiv (-1)^k \pmod{p}. \tag{21}$$

Für unseren Zweck ist es hier nicht nötig die übrigen Grössen a_i in (19) zu berechnen. Es genügt zu wissen, dass bei ihrer Berechnung keine neue Nenner eingeführt werden. Da für die zugehörigen Glieder die Faktoren $k+i+1$ im Nenner $<p$ sind, so muss nach Wegnahme von (20) der Rest von (19) eine durch p teilbare Zahl bedeuten. Hiermit ist der gewünschte Beweis erbracht, dass *für eine Primzahl* p $(k,h)_p$ *durch* p *teilbar ist oder nicht, je nachdem man* $k+h=p$ *oder* $<p$ *hat.* Man sieht auch ein, dass unter den beiden Bestandteilen von $(k,h)_p$ (15) immer durch p teilbar ist; für (14) gilt dagegen, falls $k+h=p$, die Kongruenz (21).

Als Beispiel behandeln wir zuletzt den Fall $h=3$. Nach (13) hat man hier für (15):

$$\sum_{n=k}^{n=p-1} \frac{(n+1)n(n-1)\cdots(n-k+1)}{\underline{|k-1}\cdot(k+1)}. \tag{15}'$$

Die Berechnung hiervon lässt sich unmittelbar ausführen, und zwar bekommt man:

$$\frac{(p+1)\,p\,(p-1)\cdots(p-k)}{\lfloor k-1\cdot(k+1)(k+2)}. \tag{22}$$

Es bleibt noch übrig die Behandlung von (14). Als Ausgangspunkt haben wir:

$$\sum_{n=k}^{n=p-1} \frac{n\,(n-1)\cdots(n-k+1)}{\lfloor k}\,\frac{n\,(n-1)}{2}. \tag{14'}$$

Für den letzten Faktor erhalten wir die Entwicklung:

$$\frac{n\,(n-1)}{2} = \frac{(n+1)\,(n+2)}{2} - 2\,(n+1) + 1. \tag{23}$$

Hieraus ergibt sich als Summe von (14)':

$$\frac{(p+2)\,(p+1)\,p\cdots(p-k)}{\lfloor k\cdot 2\cdot(k+3)} - \frac{2\,(p+1)\,p\cdots(p-k)}{\lfloor k\cdot(k+2)} + \frac{p\cdots(p-k)}{\lfloor k\cdot(k+1)}. \tag{24}$$

Nimmt man z. B. $k=4$ und $p=7$, so bekommt man bzw. für (22) und (24) 112 und $540-280+21=281$, also insgesamt 393, und man hat $393 \equiv (-1)^4 = 1$ (mod. 7).

Tryckt den 22 juni 1950

Uppsala 1950. Almqvist & Wiksells Boktryckeri AB