# Über eine Eigenschaft der additiven Zerfällungen der Zahlen.

Von **S. Bergmann** in Wien.

Im Vorliegenden soll die Eigenschaft der Funktion $B(n)$, die gleich dem Unterschied der Anzahlen ist, welche anzeigen, wie oft die Zahl $n$ aus einer geraden und wie oft aus einer ungeraden Anzahl verschiedener der Zahlen $1, 2, 3 \ldots (p-2)$ additiv gebildet werden kann, untersucht werden. Wenn wir das Produkt

$$f(x) = (x-1)(x^2-1)(x^3-1)\ldots(x^{p-2}-1)$$

(wobei $p$ eine Primzahl bedeutet) nach Potenzen von $x$ ordnen, ergibt sich die Reihe

$$\sum_{n=1}^{n=\frac{(p-1)(p-2)}{2}} B(n)\, x^n$$

wo $B(n)$ die angegebene Bedeutung hat. Da es sich um eine Kongruenz-Eigenschaft handelt und unter $x$ in Folgendem stets ganze Zahl verstanden wird, so dürfen wir

$$x^{s(p-1)+k} \equiv x^k \qquad (p)^{1)}$$

setzen, somit

$$f(x) \equiv x^{p-1}\left\{1 + B(p-1) + B(2p-2) + \ldots B\left[\frac{p-1}{2}(p-3)\right]\right\} +$$

$$+ x^{p-2}\left\{B(p-2) + B(2p-3) + \ldots + B\left[\frac{p-1}{2}(p-3)-1\right]\right\} +$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$+ x\left\{B(1) + B(p) + B(2p-1) + \ldots + B\left[\frac{p-1}{2}(p-3)+1\right]\right\}.$$

---

[1]) Der Modul $p$ der Kongruenz ist im folgenden nicht mehr besonders angegeben.

Darin ist jeder Klammerausdruck gleich der Summe der Werte der Funktion $B$ für Argumente gleich den Gliedern der arithmetischen Progression

$$s,\, s+p-1, \ldots s+\left(\frac{p-1}{2}\right)(p-3), \quad \text{wenn} \quad s \leqq \frac{p-1}{2},$$

$$s,\, s+p-1, \ldots s+(p-1)\left(\frac{p-5}{2}\right), \quad \text{wenn} \quad s > \frac{p-1}{2}.$$

Anderseits besitzt $f(x)$ die Eigenschaft, daß sie kongruent 1 ist, wenn $x$ gleich einer Primitivwurzel von $p$ ist (da kein

$$x^r \equiv 1$$

ist, so verwandelt sich $f(x)$ in das Produkt $1.2.3\ldots(p-2)$, welches nach Wilsonschem Satz kongruent 1 ist). Ist $x$ gleich einer Nichtprimitivwurzel von $p$, so existiert mindestens ein $x$, bei welchen

$$(x^r - 1) \equiv 0$$

und somit auch

$$f(x) \equiv 0$$

ist. Da für jede $f(x)$ die Beziehung gilt,

$$f(x) \equiv -\left[x^{p-1} \sum_{r=1}^{r=p-1} f(r) + x^{p-2} \sum_{r=1}^{r=p-1} r f(r) + \ldots \right.$$

$$\left. \ldots + x \sum_{r=1}^{r=p-1} r^{p-2} f(r)\right]^{1)},$$

so ist in unserem speziellen Falle

$$f(x) \equiv -\left[S_0\, x^{p-1} + S_1\, x^{p-2} + \ldots + S_{p-2}\, x\right],$$

wobei unter $S_k$ die Summe der $k$ Potenzen aller Primitivwurzeln von $p$ gemeint wird. Es ist nämlich nach dem Gesagten entweder $f(r) \equiv 1$ oder $f(r) \equiv 0$, je nachdem, ob $r$ eine Primitivwurzel oder Nichtprimitivwurzel ist, und somit ist also

$$\sum_{r=1}^{r=p-1} r^k f(r) \equiv S_k.$$

Ist $p-1 = m = m' P$ eine beliebige positive ganze Zahl, $P$ das Produkt aus allen von einander verschiedenen in $m$ aufgehenden

[1]) Siehe über die „analytische Darstellung der Lösungen von Kongruenzen". Monatshefte für Mathematik und Physik, XXVIII. Jahrg. 1917, S. 121.

Primzahlen und $S_k$ die Summe der $k$ Potenzen aller Primitivwurzeln von $p$, so ist $S_k = 0$, wenn $k$ nicht durch $m'$ teilbar ist; ist aber

$$k = m' K$$

ferner $Q$ der größte gemeinschaftliche Divisor von $K$ und $P (= Q R)$, und $r$ die Anzahl der in $R$ aufgehenden Primzahlen, so ist

$$S_k \equiv (-1)^r m' \varphi(Q)$$ [1]

$\varphi$-Eulersche Funktion. Da schließlich die Koeffizienten bei gleichen Potenzen von $x$ in beiden Entwicklungen der $f(x)$ übereinstimmen müssen, so ergibt sich, daß

$$B(p-s) + B(2p-s-1) + \ldots + B\left[(p-s) + (p-1)\left(\frac{p-3}{2}\right)\right] \equiv$$
$$\equiv -S_{s-1} \equiv -(-1)^r m' \varphi(Q).$$

Wenn $p - s \leqq \frac{p-1}{2}$, und

$$B(p-s) + B[(p-s) + (p-1)] + \cdots +$$
$$+ B\left[(p-s) + (p-1)\left(\frac{p-5}{2}\right)\right] \equiv -S_{s-1} \equiv -(-1)^r m' \varphi(Q),$$

wenn

$$p - s > \frac{p-1}{2}.$$

Beispiel:

$$p = 7$$

$$(x-1)(x^2-1)(x^3-1)(x^4-1)(x^5-1) = x^{15} - x^{14} - x^{13} + x^{10} +$$
$$+ x^9 + x^8 - x^7 - x^6 - x^5 + x^2 + x - 1 \equiv -x^5 + x^4 +$$
$$+ 2x^3 - x^2 - x - 2 \tag{7}$$

$$B(15) + B(9) + B(3) = -S_3 \equiv \varphi\,[\text{gr. gem. Teiler}\,(6, 3)] = \varphi(3) = 2$$
$$15 = 1 + 2 + 3 + 4 + 5 \quad 9 = 2 + 3 + 4 = 1 + 3 + 5 = 4 + 5$$
$$3 = 3 = 1 + 2$$

Also zwei Zerfällungen in gerade und vier Zerfällungen in ungerade Anzahl von Gliedern.

Außerdem folgt noch aus dem Gesagten:

Da

$$[f(x)]^k \equiv f(x)$$

ist, so dürfen wir, ohne das Resultat zu verändern, das Produkt

$$f(x) = \prod_{n=1}^{n=p-2} (x^n - 1)$$

[1] Dirichlet, Vorlesungen über Zahlentheorie, Supplement 7, 2. Aufl., S. 401 (Fußbemerkung).

zu der $k^{\text{ten}}$ Potenz erheben, d. h.: wenn wir die Unterschiede der Anzahlen, welche anzeigen, wie oft die Zahl $n$ aus einer geraden und wie oft aus einer ungeraden Anzahl der Zahlen

$$1,\ 2,\ 3, \ldots (p-2)$$

additiv gebildet werden kann (wobei in jeder Zerfällung jede Zahl höchstens $k$ mal vorkommen darf), berechnen und deren Summe für die Werte $n =$

$$s,\ s+(p-1), \ldots s+(p-1)\left[(k-1)\left(\frac{p-1}{2}\right)+\frac{p-5}{2}\right]$$

resp. $s,\ s+(p-1), \ldots s+(p-1)\left[(k-1)\left(\frac{p-1}{2}\right)+\frac{p-3}{2}\right]$

bilden, so ist sie

$$\equiv -(-1)^r m' \varphi(Q)$$

Die erwähnte Zerfällung in die Zahlen der Reihe

$$1, 2, 3 \ldots (p-2),$$

wo jede höchstens $k$-mal vorkommen kann, dürfen wir auch auffassen, als Zerfällungen in die Form

$$s = 1x_1 + 2x_2 + 3x_3 + \ldots + (p-2)x_{p-2},$$

wo für $x = 0$ oder eine beliebige Zahl, die $\leq k$ ist, genommen werden kann. Anstatt der früher angegebenen Differenz der Darstellungen mit geraden und ungeraden Anzahl der Glieder, müssen wir den Unterschied der Anzahl der Zerfälluugen bilden, wo

$$x_1 + x_2 + \ldots + x_{p-2}$$

gerade oder ungerade Zahl ist.

Die Beziehung

$$s \equiv x_1 + x_2 + \ldots + x_q \qquad (p-1)$$

dürfen wir auch in der Form

$$a^s \equiv a^{x_1} a^{x_2} \ldots a^{x_q} \quad (p) \quad (a \text{ Primitivwurzel})$$

schreiben. Da alle

$$x_1, x_2 \ldots$$

ein vollständiges Restsystem $(p-1)$ ausgenommen, modulo $(p-1)$ bilden; so bilden die Werte

$$a^{x_1}, a^{x_2}, \ldots$$

ein vollständiges Restsystem, die 1 von demselben ausgenommen, modulo $p$. Setzen wir $a^s = S$, so ist nach früher Gesagtem die Summe der Differenzen der Darstellungen der Zahlen $S+$ diejenige, von $(p+S)+$ diejenige von $(S+2p)+$ usw., als

Produkt der geraden und ungeraden Anzahl voneinander verschiedenen Multiplikatoren der Reihe

$$2, 3, 4 \ldots (p-1),$$

kongruent $-(-1)^r m' \varphi(Q)$, wo $Q$ der größte gemeinschaftliche Teiler von $p$ und $k\,m'$, $K = \text{ind.}\, S_k$ ist. Die anderen Buchstaben behalten die alte Bedeutung: $p-1 = m' P$. $P$ das Produkt aus allen voneinander verschiedenen in $(p-1)$ aufgehenden Zahlen.

Auf ganz ähnliche Weise läßt sich die Darstellung der Funktion

$$\prod_{n=1}^{n=p-1} (x^n + 1)$$

in der Form eines Polynomes $(p-1)$ Grades durchführen und somit gewisse Schlüsse über die Anzahl der Zerfällungen der Zahl $n$ aufstellen. Da aber die Formeln für den allgemeinen Fall gewisse Komplikationen erleiden, soll im folgenden der Fall durchgeführt werden, bei welchem

$$p - 1 = 2\,p_1$$

ist, wo $p_1$ wieder eine Primzahl bedeutet. Wir werden den Fall in anderer Hinsicht verallgemeinern, indem wir anstatt des früheren Produktes das Produkt

$$g(x) = \prod_{n=1}^{n=p-1} (x^n - y)$$

nehmen. Wir werden auch hier die früher erwähnte Darstellung

$$g(x) = -\left[x^{p-1} \sum_{r=1}^{r=p-1} g(r) + x^{p-2} \sum_{r=1}^{r=p-1} r\, g(r) + \ldots + x \sum_{r=1}^{r=p-1} r^{p-2}\, g(r)\right]$$

anwenden. Um die

$$\sum_{r=1}^{r=p-1} \left| r^s\, g(r) \right|$$

zu berechnen, müssen wir zuerst den Wert $g(x)$ für alle $x$ auffinden. Dazu setzen wir anstatt $x$ $a^{\text{ind.}\, x}$, anstatt $y$ $a^{\text{ind.}\, y}$ ($a$ eine Primitivwurzel von $p$) und erhalten dadurch:

$$g(x) = \prod_{n=1}^{n=p-1} (a^{n\,\text{ind.}\, x} - a^{\text{ind.}\, y}).$$

Da $n$ alle Werte

$$1, 2, \ldots p-1$$

annimmt, so verschwindet $g(x)$, sobald die Gleichung

$$n\,\text{ind.}\, x - \text{ind.}\, y \equiv 0 \quad (p-1) \quad (n \text{ variable})$$

eine Lösung besitzt. Das ist nicht der Fall, nur dann, wenn ind. $y$ durch den größten gemeinschaftlichen Teiler von $(p-1)$ und ind. $x$, nicht teilbar ist. Da $(p-1) = 2p_1$ ist, so kann der größte gemeinschaftliche Teiler entweder $\frac{p-1}{2}$, $p-1$ oder 2 sein. In beiden ersten Fällen ist

$$g(x) \equiv (1 - a^{2\,\text{ind.}\,y})^{\frac{p-1}{2}}$$

resp.

$$g(x) = (1 - a^{\text{ind.}\,y})^{p-1}$$

weil

$$a^{\frac{p-1}{2}} \equiv \pm 1, a^{p-1} \equiv 1$$

ist. Im letzten Falle verwandeln wir

$$g(x) \equiv \prod_{n=1}^{n=p-1} (a^{n\,\text{ind.}\,x} - a^{\text{ind.}\,y})$$

in

$$\prod_{n=1}^{n=p-1} (a^{n\,\text{ind.}\,x - \text{ind.}\,y} - 1.)$$

Der Ausdruck

$$a^{n\,\text{ind.}\,x - \text{ind.}\,y}$$

(ind. $x$ gerade, ind. $y$ ungerade Zahl) ergibt für

$$n = 1, 2 \ldots \quad (p-2)$$

eine Reihe, die, von der Reihefolge der Glieder abgesehen, mit der zweimal wiederholten Folge der quadratischen Nichtreste der Zahl $p$ übereinstimmt. Da nunmehr

$$g(x) \equiv \prod [(N_i - 1)]^2 \qquad \begin{array}{c} N_i\text{-quadrat. Nichtrest} \\ i = 1, 2 \ldots \frac{p-1}{2} \end{array}$$

ist. So ist auch

$$g(x) \equiv \Big\{(N_1 N_2 N_3 \ldots) - (N_1 N_2 \ldots N_{\frac{p-1}{2}} - 1 + \cdots) +$$

$$+ \ldots + (N_1 + N_2 + N_3 + \ldots) - 1\Big\}^2$$

Nun ist

$$N_1 N_2 N_3 \ldots \equiv -1$$

die anderen Summen dagegen (wie leicht aus der Theorie der symmetrischen Funktionen und aus der Beziehung

$$\Sigma N_i^s \equiv 0$$

sobald

$$\frac{p-1}{2} > s > 0$$

nachzuweisen ist) kongruent 0 sind, somit

$$g(x) \equiv (-1-1)^2 = 4.$$

Nachdem die Berechnung der Werte von $g(x)$ für alle $x$ erledigt ist, gehen wir zur Berechnung der

$$\sum_{r=1}^{r=p-1} r^k g(r).$$

Jetzt müssen wir dem ind. $y$ bestimmte Werte beilegen.

I. Ist ind. $y = (p-1)$, so kommen wir zu dem trivialen Fall, daß $g(x)$ für jedes $x$ gleich 0 ist und $g(x)$ identisch ist $\equiv 0$. Es sei noch erwähnt, daß dieser Fall eigentlich schon früher erörtert wurde, mit dem Unterschiede, daß das Produkt früher von $n=1$ bis $n=(p-2)$ jetzt von $n=1$ bis $n=(p-1)$ genommen worden ist, weshalb wir auch zu anderen Resultaten gekommen sind.

II. Ist ind. $y = \frac{p-1}{2}$; so haben wir den Fall, welchen wir eigentlich zu untersuchen haben, da

$$a^{\frac{p-1}{2}} \equiv -1,$$

und

$$\left(x^n - a^{\frac{p-1}{2}}\right) \equiv (x^n + 1).$$

Laut den früher Gesagten

$$\begin{aligned} g(x) &\equiv 0, \quad \text{wenn ind. } x - \text{ ungerade Zahl,} \\ &\equiv 4, \quad \text{wenn ind. } x - \text{ eine gerade Zahl (nicht } p-1), \\ &\equiv 1, \quad \text{wenn ind. } x - (p-1), \end{aligned}$$

somit

$$\sum_{r=1}^{r=p-1} r^s g(r) = 4\,(a^{2s} + a^{4s} + \ldots + a^{(p-3)s}) + a^{(p-1)s}1.$$

Für $s = (p-1)$ oder $\left(\frac{p-1}{2}\right)$

ist $$\sum_{r=1}^{r=p-1} r^s g(r) \equiv 4\,\frac{p-3}{2} + 1 = -6 + 1 = -5$$

für alle anderen $s = 1 + 4 \frac{a^{(p-1)s} - a^{2s}}{a^{2s} - 1} = -4 + 1 = -3.$

Somit ergibt schließlich unsere Zerlegung:

$$g(x) = 5\,x^{p-1} + 3\,x^{p-2} + 3\,x^{p-3} + \ldots + 3\,x^{\frac{p-1}{2}+1} +$$
$$+ 5\,x^{\frac{p-1}{2}} + 3\,x^{\frac{p-1}{2}-1} + \ldots + 3\,x$$

III. Ist weiter ind. $y$ eine andere gerade Zahl, so ist

$$\sum_{r=1}^{r=p-1} r^s\, g(r) = (-1)^s (1 - y^2)^{\frac{p-1}{2}} + 1.$$

IV. Ist schließlich ind. $y$ eine ungerade Zahl und nicht gleich $\left(\frac{p-1}{2}\right)$

$$\sum r^s\, g(r) = -3 + (-1)^s (1 - y^2)^{\frac{p-1}{2}}$$

für $s =$ einer geraden Zahl (nicht $p - 1$);

$$= -5 + (-1)^s (1 - y^2)^{\frac{p-1}{2}}$$

für $s = \frac{p-1}{2}$ oder $p - 1$

$$= 1 + (-1)^s (1 - y^2)^{\frac{p-1}{2}}$$

für $s =$ einer anderen ungeraden Zahl.

Aus der früher durchgeführten Zerlegung

$$\prod_{n=1}^{n=p-1} (x^n + 1) = 5\,x^{p-1} + 3\,x^{p-2} + \ldots + 3\,x^{\frac{p-1}{2}+1} + 5\,x^{\frac{p-1}{2}} +$$
$$+ 3\,x^{\frac{p-1}{2}-1} + \ldots + 3\,x$$

können wir nun schließen, daß die Summe der Anzahlen der Zerfällungen der Zahlen einer arithmetischen Progression

$$k, k + (p-1), \ldots k + (p-1)\left(\frac{p-1}{2}\right)$$

wenn $$k \leqq \frac{p-1}{2},$$

$$k, k + (p-1), \ldots k + (p-1)\left(\frac{p-3}{2}\right),$$

wenn
$$k > \frac{p-1}{2}$$

entweder $\equiv 5$ ist, wenn $k = \frac{p-1}{2}$ oder $p - 1$ ist,

$\equiv 3$ in allen übrigen Fällen,

wobei wir noch einmal hervorheben wollen $\left(\frac{p-1}{2}\right) = p_1$, wo $p$ und $p_1$ beide Primzahlen sein müssen.

Beispiel: $p = 11$ [$A(s)$ — Anzahl der Zerfällungen von $s$]

$$A(5) + A(15) + A(25) + A(35) + A(45) + A(55) = \\ = 3 + 20 + 39 + 31 + 10 + 1 = 104 \equiv 5 \qquad (11)$$

Nun dürfen wir auch jetzt einige unsere früheren Schlüsse hier wiederholen:

Summe der Anzahlen der Zerfallungen der Zahlen

$$k, \; k + p - 1 \ldots$$

in Summen, wo jeder Summand höchstens $s$-mal vorkommen darf, ist

$$\equiv 3 \quad \text{oder} \quad 5;$$

auch die Summen der Darstellungen der Zahlen

$$k, \; k + p - 1, \ldots$$

in der Form

$$1\, x_1 + 2\, x_2 \ldots + (p-1)\, x_{p-1},$$

wo
$$x \leq s$$

ist $\equiv$

$$3 \quad \text{oder} \quad 5.$$