Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$.

Von PAUL ERDÖS in Manchester und RICHARD OBLÁTH in Budapest.

Einleitung.

Man hat bereits öfters vermutet, jedoch bisher allgemein nicht bewiesen[1]), daß die unbestimmten Gleichungen

(I) $$n! = x^p + y^p \qquad (p > 1)$$

und

(II) $$n! = x^p - y^p \qquad (p > 2)$$

außer der trivialen Lösung $x = y = 1$, $n = 2$ von (I) keine Lösung in positiven ganzen Zahlen x, y, p, n zulassen. Ohne Beschränkung der Allgemeinheit darf man annehmen, daß in (I) p eine Primzahl bzw. in (II) $p = 4$ oder p eine Primzahl ist. Der Fall $p = 2$ von (I) d. h. die Gleichung

(Ia) $$n! = x^2 + y^2$$

ist leicht zu erledigen[2]), da es zwischen $\frac{n}{2}$ und n für $n \geqq 7$ stets

[1]) Betreffend der Literatur dieser Frage vgl. L. DICKSON, *History of the Theory of Numbers*, Vol. II: *The Diophantine Analysis* (Washington, 1919), pp. 681, 682. Außer den daselbst zitierten Arbeiten sind uns noch die beiden folgenden Mitteilungen bekannt: A. GÉRARDIN, Question 597, *Mathesis*, (3) **6** (1906), pp. 218—219 und A. FLECHSENHAAR, Aufgabe 455, *Zeitschrift für math. und naturwiss. Unterricht*, **45** (1919), p. 440. Beide ohne nennenswertes Resultat.

H. BROCARD, Question 2999, *Intermédiaire des math.*, **13** (1906), p. 130, sagt ausdrücklich, daß er lange vergeblich einen Beweis gesucht hat.

Bemerkung bei der Korrektur. Nachträglich erhielten wir Kenntnis von der folgenden Arbeit: H. GUPTA, On the Diophantine Equation $m^2 = n! + 1$, *American Math. Monthly*, **43** (1936), p. 32—34. Sie enthält nur numerische Rechnungen.

[2]) Für $y = 1$ steht dies bei FLECHSENHAAR, a. a. O. [1]).

eine Primzahl q der Form $4k+3$ gibt[3]); da nun $n!$ durch q, nicht aber durch q^2 teilbar ist, so ist (Ia) für $n \geqq 7$ unmöglich (und auch für $n=3, 4, 5$, wegen $3|n!$, $9 \nmid n!$). Es ist jedoch $6! = 12^2 + 24^2$.

Wir beschränken unsere Untersuchung auf den Fall, daß x und y teilerfremd sind. Wir beweisen dann in § 2, daß (I) und (II), außer der erwähnten trivialen, keine Lösung besitzen, falls p eine ungerade Primzahl bedeutet, also auch dann nicht, falls p eine beliebige ungerade Zahl oder auch eine Zahl bedeutet, die keine Potenz von 2 ist.

Die Hauptstütze unseres Beweises bildet die Formel (V), welche eine Abschätzung des Beitrages der Primzahlen von der Form $2kp+1$ zur Primfaktorendarstellung von $n!$ liefert. Diese Formel beweisen wir in § 1 durch dieselbe Methode, welche einer von uns für die Abschätzung des Produktes der in einer beliebigen arithmetischen Reihe enthaltenen Primzahlen unter einer gegebenen Grenze entwickelt hat[4]). Der Primzahlsatz[5]) würde allerdings schärfere Abschätzungen liefern; die hier angewandte Methode besitzt aber außer ihrem elementaren Charakter den Vorzug, Resultate zu liefern, die von Anfang an gültig sind, während bekanntlich die Bestimmung des Geltungsbereiches einer aus dem Primzahlsatze gewonnenen numerischen Abschätzung langes Rechnen erfordert[6]).

Durch dieselbe Methode werden wir im § 3 die Unlösbarkeit der Gleichung (II) für $p=8$, d. h. von

(IIa) $$n! = x^8 - y^8$$

beweisen (woraus natürlich die Unlösbarkeit von (II) für $p=2^\alpha$, $\alpha \geqq 3$ folgt).

Für $p=4$, d. h. bei der Gleichung

(IIb) $$n! = x^4 - y^4$$

[3]) R. Breusch, Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und $2x$ stets Primzahlen liegen, *Math. Zeitschrift*, **34** (1932), pp. 505—526; P. Erdös, Über die Primzahlen gewisser arithmetischer Reihen, *Math. Zeitschrift*, **39** (1935), pp. 473—491.

[4]) P. Erdös, a. a. O. [3]), insbesondere p. 485, Formel (12). *Die hier gegebene Abschätzung ist jedoch etwas schärfer.* Siehe auch G. Ricci, Sul teorema di Dirichlet relativo alla progressione aritmetica, *Bolletino dell'Unione Mat. Italiana*, **12** (1933), pp. 304—309.

[5]) Unter „Primzahlsatz" wird stets der auf die entsprechende arithmetische Reihe bezügliche Primzahlsatz verstanden.

[6]) Siehe z. B. bei Breusch, a. a. O. [3]).

versagt hingegen die erwähnte Formel (V). Der Unmöglichkeitsbeweis dieser Gleichung erfordert nämlich so genaue Kentnisse über die Verteilung der Primzahlen unter den beiden arithmetischen Reihen $4k+1$ und $4k+3$, wie sie derzeit nur der Primzahlsatz[5]) liefern kann. Daher können wir die Unlösbarkeit der Gleichung (IIb) nur für hinreichend große n beweisen. § 4 enthält einen hierzu nötigen Hilfssatz aus der analytischen Zahlentheorie, § 5 den Unlösbarkeitssatz.

Im § 6 beschäftigen wir uns mit einem Problem, das gewissermaßen als Gegenstück des ersten betrachtet werden kann. Wir werden nämlich, ebenfalls mit Hilfe des (gewöhnlichen) Primzahlsatzes beweisen, daß die unbestimmten Gleichungen

$$(III) \qquad n! \pm m! = x^p \qquad (n > m > 1,\ p > 1)$$

höchstens endlich viele Lösungen zulassen.

Die beiden Resultate können kurz und frappant etwa so formuliert werden: *Faktorialzahlen sind* (im allgemeinen) *keine Potenzsummen* oder Potenzdifferenzen und *Summen* oder Differenzen *zweier Faktorialzahlen sind* (im allgemeinen) *keine vollen Potenzen.*

§ 1. Abschätzung des Beitrages gewisser Primfaktoren zu $n!$.

Nach einem klassischen Satz von LEGENDRE lautet der Exponent einer Primzahl q in der Zerlegung der Zahl $n!$ in Primfaktoren

$$(1) \qquad u(n, q) = \left[\frac{n}{q}\right] + \left[\frac{n}{q^2}\right] + \left[\frac{n}{q^3}\right] + \dots$$

Also ist der Beitrag aller in einer arithmetischen Progression $ak+b$ $((a, b) = 1,\ 0 < b < a)$ enthaltenen Primzahlen zur Primfaktorendarstellung von $n!$

$$T(n, a, b) = \prod_{\substack{q \equiv b \pmod a \\ q \text{ Primzahl}}} q^{u(n, q)} = \prod_{\substack{q \equiv b \pmod a \\ q \text{ Primzahl}}} \prod_{r=1}^{\infty} q^{\left[\frac{n}{q^r}\right]}.$$

Wir werden diesen Ausdruck ähnlicherweise umformen, wie es bei Ableitung der Tschebyscheff—de Polignacschen Identität[7]) mit

[7]) E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlen* (Leipzig und Berlin, 1909), I, p. 87.

$n!$ geschieht. Der Bequemlichkeit der Schreibweise halber gehen wir zu den Logarithmen über[8]):

$$\log T(n,a,b) = \sum_{\substack{q\equiv b \pmod a \\ q \text{ Primzahl}}} \sum_{r=1}^{\infty} \left[\frac{n}{q^r}\right] \log q =$$

$$= \sum_{\substack{q\equiv b \pmod a \\ q \text{ Primzahl}}} \sum_{r=1}^{\infty} \sum_{s\leqq \frac{n}{q^r}} \log q = \sum_{s=1}^{\infty} \sum_{r=1}^{\infty} \sum_{\substack{q\equiv b \pmod a \\ q\leqq \sqrt[r]{n/s} \text{ Primzahl}}} \log q,$$

also ist, wenn man

$$\Psi(x,a,b) = \prod_{r=1}^{\infty} \prod_{\substack{q\equiv b \pmod a \\ q\leqq \sqrt[r]{x} \text{ Primzahl}}} q = \prod_{q\leqq x} q \prod_{q\leqq \sqrt{x}} q \prod_{q\leqq \sqrt[3]{x}} q \ldots$$

setzt (wobei q die in der arithmetischen Reihe $ak+b$ enthaltenen Primzahlen durchläuft),

$$(2) \qquad T(n,a,b) = \prod_{s=1}^{\infty} \Psi\left(\frac{n}{s}, a, b\right) =$$

$$= \Psi(n,a,b)\, \Psi\left(\frac{n}{2}, a, b\right)\, \Psi\left(\frac{n}{3}, a, b\right) \ldots$$

Nun beschränken wir uns, im Einklang mit unserem Ziele, auf den Spezialfall $b=1$ und schreiben statt $T(n,a,1)$ und $\Psi(x,a,1)$ kürzer $T(n,a)$ bzw. $\Psi(x,a)$. Wir werden $\Psi(x,a)$ von oben abschätzen; daraus gewinnen wir dann mit Hilfe von (2) eine Abschätzung von $T(n,a)$.

Zu diesem Zwecke untersuchen wir den Ausdruck[9])

$$P(m,a) = \prod_{\substack{p\mid a \\ p \text{ Primzahl}}} p^{\left[\frac{m-1}{p-1}\right]} \frac{(a+1)(2a+1)\ldots((m-1)a+1)}{m!},$$

wobei m eine beliebige positive ganze Zahl sein kann. Wegen

$$\frac{ka+1}{k+1} \leqq a \qquad (k=1,2,\ldots,m-1)$$

ergibt sich unmittelbar die Abschätzung

$$(3) \qquad P(m,a) \leqq \prod_{\substack{p\mid a \\ p \text{ Primzahl}}} p^{\frac{m-1}{p-1}} a^{m-1} = A^{m-1}$$

---

[8]) Sämtliche Umformungen sind gestattet, da die Reihen nur scheinbar unendlich sind.

[9]) Identisch mit $P'_m(a,1)$ bei Erdős, a. a. O. [3]).

mit

$$A = A(a) = a \prod_{\substack{p \mid a \\ p \text{ Primzahl}}} p^{\frac{1}{p-1}}. \tag{4}$$

Ferner ist $P(m, a)$ eine ganze Zahl. In der Tat kommt eine Primzahl q in der Primfaktorendarstellung von $(a+1)(2a+1)\ldots((m-1)a+1)$ offenbar mit dem Exponenten

$$v(m, q) = v_1(m, q) + v_2(m, q) + v_3(m, q) + \ldots \tag{5}$$

vor, wobei $v_r(m, q) = v_r(m, q, a)$ die Anzahl der Lösungen der Kongruenz $q^r x \equiv 1 \pmod a$ mit der Nebenbedingung $1 \leqq q^r x \leqq (m-1)a+1$ oder, was auf dasselbe hinauskommt, $0 < q^r x \leqq ma$ bedeutet. Für x steht also das Intervall $1 \leqq x \leqq \left[\frac{ma}{q^r}\right]$ zur Verfügung; wegen $\left[\frac{ma}{q^r}\right] \geqq a\left[\frac{m}{q^r}\right]$ enthält dieses Intervall jedenfalls $\left[\frac{m}{q^r}\right]$ vollständige Restsysteme mod a; ist $(q, a) = 1$, so ist daher

$$v_r(m, q) \geqq \left[\frac{m}{q^r}\right] \qquad (r = 1, 2, 3, \ldots), \tag{6}$$

also wegen (1) und (5)

$$v(m, q) \geqq u(m, q),$$

d. h. die zu a teilerfremden Primzahlen q kommen im Zähler von $P(m, a)$ mindestens in derselben Multiplizität vor, wie im Nenner. Das Gleiche gilt aber auch für die Primzahlen $q \mid a$ wegen

$$(q-1)\,u(n, q) < (q-1)\left(\frac{n}{q} + \frac{n}{q^2} + \frac{n}{q^3} + \ldots\right) = n,$$

woraus sich wegen der Ganzzahligkeit von $u(n, q)$

$$(q-1)\,u(n, q) \leqq n-1, \quad u(n, q) \leqq \frac{n-1}{q-1}, \quad u(n, q) \leqq \left[\frac{n-1}{q-1}\right]$$

ergibt.

Es sei nun q eine Primzahl von der Form $ak+1$, die einem der Intervalle $m < q < ma+1, \sqrt{m} < q < \sqrt{ma+1}, \sqrt[3]{m} < q < \sqrt[3]{ma+1}, \ldots$ angehört. Diese Intervalle können sich zwar teilweise überdecken; doch kann q nicht dem Durchschnitt zweier dieser Intervalle angehören, da aus $\sqrt[r]{m} < q < \sqrt[r+1]{ma+1}$

$$q=\frac{q^{r+1}}{q^r}<\frac{ma+1}{m}\leqq a+1$$

folgen würde, während offenbar $q\geqq a+1$.

Ist nun $\sqrt[s]{m}<q<\sqrt[s]{am+1}$, so ist offenbar $v_s(m,q)=1$, $\left[\frac{m}{q^s}\right]=0$, also wegen (1), (5) und (6)

$$v(m,q)>u(m,q),$$

d. h. $P(m,a)$ ist durch q teilbar. Also ist

$$Q(m,a)=\prod_{r=1}^{\infty}\prod_{\substack{\sqrt[r]{m}<q<\sqrt[r]{am+1}\\ q\equiv 1 \pmod a\\ q\text{ Primzahl}}}^{r} q=$$

$$=\prod_{m<q<am+1} q\prod_{\sqrt{m}<q<\sqrt{am+1}} q\prod_{\sqrt[3]{m}<q<\sqrt[3]{am+1}}^{3} q\ldots$$

(wobei q — wie auch weiter unten in diesem Paragraphen — die Primzahlen von der Form $ak+1$ durchläuft) ein Teiler von $P(m,a)$; wegen (3) ist also

$$Q(m,a)\leqq A^{m-1}.$$

Ersetzen wir hier die Zahl m der Reihe nach durch

$$m_1=\left\{\frac{m}{a}\right\},\quad m_2=\left\{\frac{m}{a^2}\right\},\ldots,\quad m_s=\left\{\frac{m}{a^s}\right\}=1\qquad (a^{s-1}<m\leqq a^s),$$

wobei $\{t\}$ die kleinste ganze Zahl $\geqq t$ bezeichnet, und multiplizieren wir die so entstandenen Ungleichungen, so gewinnen wir wegen

$$am_{r+1}+1\geqq a\frac{m}{a^{r+1}}+1=\frac{m}{a^r}+1>m_r$$
$$(r=0,1,2,\ldots,s-1;\ m_0=m)$$

die Ungleichung

$$\text{(7)}\qquad \prod_{r=1}^{\infty}\prod_{q<\sqrt[r]{am+1}}^{r} q\leqq Q(m,a)\,Q(m_1,a)\,Q(m_2,a)\ldots Q(m_s,a)\leqq$$
$$\leqq A^{m+m_1+m_2+\ldots+m_s-s-1}.$$

Nun ist aber $q<\sqrt[r]{am+1}$ mit $q^r<am+1$, $q^r\leqq am$, also $q\leqq\sqrt[r]{am}$ gleichbedeutend, so daß für die rechte Seite von (7) $\Psi(am,a)$ geschrieben werden kann; ferner ist

$$m+m_1+m_2+\ldots+m_s \leqq m+\frac{m+a-1}{a}+\frac{m+a^2-1}{a^2}+\ldots+$$

$$+\frac{m+a^s-1}{a^s}=(m-1)\left(1+\frac{1}{a}+\ldots+\frac{1}{a^s}\right)+s+1<$$

$$<(m-1)\frac{a}{a-1}+s+1,$$

was in (7) eingesetzt

$$\Psi(am, a) \leqq A^{\frac{a}{a-1}(m-1)}$$

ergibt. Zu gegebenem (nicht notwendig ganzem) $x>0$ sei m durch die Bedingung

$$a(m-1)<x \leqq am$$

bestimmt; dann erhalten wir die auch *an und für sich interessante Abschätzung*

$$\Psi(x, a) \leqq A^{\frac{x}{a-1}}. \tag{IV}$$

Als interessanter *Spezialfall* sei

$$\Psi(x, 4)=\prod_{r=1}^{\infty} \prod_{\substack{q \equiv 1 \pmod 4 \\ q \leqq \sqrt[r]{x}\ \text{Primzahl}}} q \leqq 2^x \tag{IVa}$$

hervorgehoben (in der Tat ist $A(4)=4 \cdot 2=8$).

Nun wenden wir (IV) zur Abschätzung des Beitrages $T(n, a)$ der Primfaktoren von der Form $ak+1$ zu $n!$ an. Bezeichnet q die kleinste Primzahl dieser Form und bemerkt man, daß für $x<q_0$ $\Psi(x, a)=1$ ist, so gewinnt man aus (2) $(b=1)$

$$T(n, a)=\prod_{s \leqq \frac{n}{q_0}} \Psi\left(\frac{n}{s}, a\right) \leqq A^{\frac{n}{a-1} \sum_{s \leqq \frac{n}{q_0}} \frac{1}{s}},$$

also, wegen[10]) $\sum_{s \leqq x} \frac{1}{s} \leqq \log x+1$, die gesuchte Abschätzung

$$T(n, a) \leqq A^{\frac{n}{a-1}\left(\log \frac{n}{q_0}+1\right)}. \tag{V}$$

Für die Anwendungen kommen für uns nur die beiden Spezialfälle 1) $a=2p$, p ungerade Primzahl; 2) $a=8$ in Betracht.

---

[10]) Für ganze x ergibt sich diese Ungleichung z. B. durch vollständige Induktion, und daraus auch für nicht ganze Werte.

Im ersten Falle ist nach (4)

$$A(2p) = 2p \,.\, 2 \,.\, p^{\frac{1}{p-1}} = 4p^{\frac{p}{p-1}}$$

und

$$q_0 \geqq 2p + 1 \geqq 7,$$

also

$$\text{(Va)} \qquad T(n, 2p) \leqq \left(4p^{\frac{p}{p-1}}\right)^{\frac{n}{2p-1}(\log n - \log 7 + 1)};$$

im zweiten Falle

$$A(8) = 8 \,.\, 2 = 16$$

und

$$q_0 = 17,$$

also

$$\text{(Vb)} \qquad T(n, 8) \leqq 16^{\frac{n}{7}(\log n - \log 17 + 1)}.$$

§ 2. **Der Fall einer ungeraden Primzahl** p.

Nehmen wir an, es sei

$$\text{(8)} \qquad n! = x^p \pm y^p,$$

$x > y > 0$ ganz, $(x, y) = 1$, und p eine ungerade Primzahl, ferner im Falle des Pluszeichens nicht zugleich $x = 1$, $y = 1$. Wir werden daraus einen Widerspruch ableiten.

Setzen wir

$$B_1 = x \pm y,$$

$$B_2 = \frac{x^p \pm y^p}{x \pm y} = x^{p-1} \mp x^{p-2}y + x^{p-3}y^2 \mp \ldots + y^{p-1};$$

dann ist nach (8)

$$\text{(9)} \qquad n! = B_1 B_2.$$

Bekanntlich[11]) besitzt B_2 nur Primteiler von der Form $kp + 1$, ausgenommen eventuell den Primteiler p (der auch dann nur in der ersten Potenz in B_2 enthalten sein kann). Daraus folgt, daß B_2 höchstens gleich dem p-fachen Beitrage der Primfaktoren von der Form $kp + 1$, d. h. von der Form $2kp + 1$, zu $n!$ ist:

$$\text{(10)} \qquad B_2 \leqq p\, T(n, 2p).$$

[11]) L. Euler, 1747. S. z. B. *Commentationes Arithmeticae Collectae* (Petropoli, 1849), I, p. 50. und II, p. 523. Auch in Lehrbüchern, s. z. B. G. Wertheim, *Anfangsgründe der Zahlenlehre* (Braunschweig, 1902), p. 298.

Ferner findet man leicht[12])

$$B_1^2 \leqq 4B_2. \tag{11}$$

Aus (Va), (9), (10) und (11) folgt nun einerseits

$$n!^2 = B_1^2 B_2^2 \leqq 4B_2^3 \leqq 4p^3 \left(4p^{\frac{p}{p-1}}\right)^{\frac{3}{2p-1}n(\log n - \log 7 + 1)}$$

Andererseits ist aber[13])

$$n! > 2\left(\frac{n}{e}\right)^n = 2e^{n(\log n - 1)};$$

aus den beiden Ungleichungen gewinnt man

$$\frac{2}{3}n(\log n - 1) < \log p + \tag{12}$$
$$+\frac{1}{2p-1}\left(\log 4 + \frac{p}{p-1}\log p\right)n(\log n - \log 7 + 1).$$

Um aus (12) weitere Folgerungen ziehen zu können, bemerken wir, daß notwendig $n \geqq 2p+1$ ist. Sonst wäre nämlich $n!$ durch keine Primzahl von der Form $2kp+1$ teilbar, also entweder $B_2 = 1$, oder $B_2 = p$. Im Falle des Minuszeichens in (8) gilt aber

$$B_2 = x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \ldots + y^{p-1} > p$$

außer $x = y = 1$, was keine Lösung von II liefert. Im Falle des Pluszeichens kann $B_2 = 1$, d. h.

$$x^p + y^p = x + y$$

offenbar nur im Falle der ausgenommenen trivialen Lösung $x = y = 1$ stattfinden; aus $B_2 = p$, d. h.

$$x^p + y^p = p(x+y)$$

folgt aber, wie wir sofort zeigen werden, $x = 2$, $y = 1$, $p = 3$, also $x^p + y^p = 9$, was keine Faktorialzahl ist. In der Tat, aus $x \geqq y$ folgt zunächst $y = 1$, sonst wäre $x \geqq 2$, $y \geqq 2$, $x^{p-1} > p$, $y^{p-1} > p$, $x^p + y^p > p(x+y)$; ferner gilt wegen $x \geqq 2$

---

[12]) In der Tat ist

$$(x+y)^3 \leqq (x+y)^3 + 3(x+y)(x-y)^2 = 4(x^3+y^3) \leqq 4(x^p+y^p)$$

und

$$(x-y)^2 < x^2 + xy + y^2 < x^{p-1} + x^{p-2}y + \ldots + y^{p-1}.$$

[13]) Aus der Exponentialreihe folgt nämlich ohne weiteres

$$e^n > \frac{n^{n-1}}{(n-1)!} + \frac{n^n}{n!} = 2\frac{n^n}{n!}.$$

$$\frac{x^p+1}{x+1} \geqq x^{p-1}-x^{p-2}+1 = (x-1)\,x^{p-2}+1 \geqq 2^{p-2}+1 \geqq p$$

und das Gleichheitszeichen gilt offenbar nur für $p=3$, $x=2$.

Kehren wir nun zur Ungleichung (12) zurück! Durch Differenzieren weist man unschwer nach[14]), daß die rechte Seite für $n \geqq 7$, $3 \leqq p \leqq \frac{n-1}{2}$ monoton abnimmt; daher folgt aus (12)

$$\frac{2}{3}\,n(\log n - 1) < \log 3 + \frac{1}{5}\left(\log 4 + \frac{3}{2}\log 3\right) n(\log n - \log 7 + 1).$$

Man sieht leicht, daß diese Ungleichung für $n \geqq 20$ falsch ist, also $n!^2 > 4B_2^3$ besteht. Eine numerische Nachprüfung[15]) zeigt, daß das Gleiche auch für $n \leqq 19$ der Fall ist; damit haben wir die Unmöglichkeit der Gleichung (8) ganz allgemein bewiesen. Es gilt also der

Satz 1. *Außer* $2!=2$ *läßt sich keine Faktorialzahl als Summe oder Differenz der p-ten Potenzen zweier teilerfremden Zahlen darstellen, sobald* $p \geqq 3$ *keine Potenz von* 2 *ist.*

Korollar. *Die Zahlen* $n! \pm 1$ $(n>2)$ *sind keine p-ten Potenzen.*

§ 3. Der Fall $p=8$.

Um die Unmöglichkeit der Gleichung

(IIa) $$n! = x^8 - y^8$$

$((x,y)=1)$ nachzuweisen, verfahren wir in ähnlicher Weise. Wir setzen

$$B_1 = x^4 - y^4,\quad B_2 = x^4 + y^4;$$

---

[14]) Man findet, daß die Derivierte der rechten Seite gleich

$$\frac{1}{p} - c\,\frac{2p^2-1}{(p-1)^2(2p-1)^2}\log p - c\,\frac{2(\log 4-1)p-(2\log 4-1)}{(p-1)(2p-1)^2}$$

ist, wobei $c = n(\log n - \log 7 + 1) \geqq n$. Das dritte Glied ist von Anfang an (d. h. für $p \geqq 3$) negativ, das zweite ist für $3 \leqq p \leqq \frac{n-1}{2}$ wegen $\log p > 1$, $(2p-1)^2 < 2(2p^2-1)$ absolut größer als

$$\frac{n}{2(p-1)^2} > \frac{n}{2p^2} \geqq \frac{n}{p(n-1)} > \frac{1}{p}.$$

[15]) Man beachte dabei, daß $p \leqq \frac{n-1}{2} \leqq 9$, ferner $2\cdot 7+1 = 15$ keine Primzahl ist, also nur die Fälle $p=3$ und $p=5$ in Betracht kommen. Diese Fälle erledigt man leicht mit Hilfe der Ungleichung (10).

dann folgt aus (IIa) wegen $B_1 < B_2$

$$n! = B_1 B_2 < B_2^2. \tag{13}$$

Ferner ist

$$B_2 \leqq 2T(n, 8), \tag{14}$$

da B_2 bekanntlich[16]) — eventuell vom einfachen Primfaktor 2 abgesehen — lauter Primteiler von der Form $8k+1$ besitzt. Aus (Vb), (12), (13) und $n! > 2\left(\frac{n}{e}\right)^n$ folgt nun

$$n^n e^{-n} < 2 \cdot 16^{\frac{2n}{7}(\log n - \log 17 + 1)},$$

$$n\log n - n < \log 2 + \frac{8}{7} n \log 2 (\log n - \log 17 + 1),$$

oder, nach numerischer Durchführung der Rechnungen

$$0{,}208 n \log n + 0{,}451 n < 0{,}694,$$

was ersichtlich bereits für $n \geqq 2$ unmöglich ist; für $n = 1$ hat aber (IIa) offenbar ebenfalls keine Lösung. Es besteht demnach der

Satz 2. *Die Differenz der achten Potenzen zweier teilerfremden ganzen Zahlen ist niemals eine Faktorialzahl.* Speziell ist also $n!+1$ niemals eine achte Potenz.

§ 4. Ein Hilfssatz über Charaktere.

Um unseren Satz auf vierte Potenzen ausdehnen zu können, müssen wir den befolgten Weg verlassen, denn die Primzahlen sind in den arithmetischen Reihen $4k+1$ und $4k+3$ asymptotisch gleich verteilt, es fehlt also die Grundlage, auf welche der entscheidende Schritt unserer Schlußweise sich gründete.

Tiefere Hilfsmittel führen aber auch in diesem Falle zum Ziele. Im weiteren Verlaufe unserer Untersuchung benötigen wir den folgenden

Hilfssatz. *Die Summe*

$$\sum_{q^r \leqq n}{}' \frac{\chi(q^r)\log q}{q^r}$$

ist für hinreichend großes n stets negativ; dabei bedeutet $\chi(n)$ den Nichthauptcharakter mod 4 *und q^r durchläuft bei der Summation die Primzahlpotenzen.*

[16]) Vgl. a. a. O. [11]).

Den Ausgangspunkt des Beweises bildet die bekannte, formal leicht erhältliche Identität[17])

$$(15) \qquad \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} = \sum_{\substack{q^r \\ q \text{ Primzahl}}} \frac{\chi(q^r)\log q}{q^r} \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

In der Tat sind zunächst alle drei unendliche Reihen konvergent. Für die erste und dritte Reihe ist dies evident, denn ihre Glieder haben alternierende Vorzeichen und nehmen dem absoluten Betrage nach monoton ab; die Konvergenz der mittleren Reihe folgt, wie bekannt, aus dem Primzahlsatze (für die arithmetischen Reihen $4k+1$ bzw. $4k+3$. Und umgekehrt: aus der Konvergenz folgt der Primzahlsatz). Ein klassischer Satz aus der Theorie der Dirichletschen Reihen besagt[18]), daß wenn das formale Dirichletsche Produkt zweier konvergenten Reihen wieder konvergiert, so ist die Summe der Produktreihe das Produkt der Summen der beiden Reihen.

Wegen

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n} \left(= \frac{\pi}{4}\right) > 0$$

und

$$\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} = -\left(\frac{\log 3}{3} - \frac{\log 5}{5}\right) - \left(\frac{\log 7}{7} - \frac{\log 9}{9}\right) - \ldots < 0$$

ist die Summe der Reihe $\sum_{q \text{ Primzahl}} \frac{\chi(q^r)\log q}{q^r}$ negativ, womit unser Hilfssatz bewiesen ist.

§ 5. Der Fall $p = 4$.

Um die Unmöglichkeit der Gleichung

$$(\text{IIb}) \qquad n! = x^4 - y^4$$

für hinreichend große n zu beweisen, verfahren wir wie folgt. Setzt man

$$B_1 = x^2 - y^2, \quad B_2 = x^2 + y^2,$$

so folgt

$$B_1 < B_2, \quad B_1 B_2 = n!,$$

ferner, da B_2 — vom eventuellen einfachen Primfaktor 2 abgesehen — nur durch Primzahlen von der Form $4k+1$ teilbar ist,

[17]) Vgl. LANDAU, a. a. O. [7]), p. 447.

[18]) Vgl. LANDAU, a. a. O. [7]), II, p. 765.

$$B_2 \leqq 2T(n, 4, 1)$$

und

$$B_1 \geqq 2^{u(n,2)-1} T(n, 4, 3).$$

Also folgt aus der Lösbarkeit der Gleichung (IIb)

$$2^{u(n,2)} T(n, 4, 3) < 4T(n, 4, 1),$$

d. h.

$$u(n, 2)\log 2 + \sum_{\substack{q \equiv 3 \pmod 4 \\ q \text{ Primzahl}, q^r \leqq n}} \left[\frac{n}{q^r}\right] \log q < \log 4 + \sum_{\substack{q \equiv 1 \pmod 4 \\ q \text{ Primzahl}, q^r \leqq n}} \left[\frac{n}{q^r}\right] \log q.$$

Hieraus folgt wegen

$$u(n, 2) = \sum_{r=1}^{\infty} \left[\frac{n}{2^r}\right] = \sum_{r \leqq \frac{\log n}{\log 2}} \left[\frac{n}{2^r}\right] \geqq \sum_{r \leqq \frac{\log n}{\log 2}} \frac{n}{2^r} - \left[\frac{\log n}{\log 2}\right] =$$

$$= n - \frac{n}{2^{\left[\frac{\log n}{\log 2}\right]}} - \left[\frac{\log n}{\log 2}\right] \geqq n - 1 - \frac{\log n}{\log 2}$$

die Ungleichung

$$n\log 2 - \log 8n < \sum_{\substack{q \equiv 1 \pmod 4 \\ q \text{ Primzahl} \\ q^r \leqq n}} \frac{n}{q^r} \log q - \sum_{\substack{q \equiv 3 \pmod 4 \\ q \text{ Primzahl} \\ q^r \leqq n}} \left(\frac{n}{q^r} - 1\right) \log q =$$

$$= n \sum_{\substack{q^r \leqq n \\ q \text{ Primzahl}}} \frac{\chi(q^r) \log q}{q^r} + \sum_{\substack{q \equiv 3 \pmod 4 \\ q \text{ Primzahl} \\ q^r \leqq n}} \log q.$$

Zufolge des Hilfssatzes aus § 4 ist hier die erste Summe für hinreichend grosses n negativ; die zweite Summe ist laut der Hadamardschen Form des Primzahlsatzes[19]) asymptotisch gleich $\frac{n}{2}$, woraus ein Widerspruch folgt. Wir haben somit folgenden Satz bewiesen:

[19]) Setzt man, wie üblich,

$$\Theta(n) = \sum_{\substack{q \equiv 3 \pmod 4 \\ q \text{ Primzahl} \\ q \leqq n}} \log q,$$

dann besagt jene Form des Primzahlsatzes

$$\Theta(n) \sim \frac{n}{2},$$

also auch

$$\Theta(n) + \Theta(\sqrt{n}) + \Theta(\sqrt[3]{n}) + \ldots \sim \frac{n}{2}.$$

Satz 3. *Für hinreichend großes n läßt sich $n!$ nicht als Differenz der vierten Potenzen zweier teilerfremden ganzen Zahlen darstellen.*

§ 6. Die Gleichung $n! \pm m! = x^p$.

Nehmen wir an, daß

(III) $$n! \pm m! = x^p \qquad (n > m > 1,\ p > 1),$$

dann ist $n \leqq 2m$. In der Tat gibt es infolge des Bertrandschen Postulates im Intervalle $\left(\left\{\frac{m}{2}\right\}, m\right)$ stets eine Primzahl q; q ist in $m!$ offenbar in der ersten Potenz enthalten. Wäre $n > 2m \geqq 2q$, so würde $n!$ durch q^2 teilbar sein; dann wäre aber $n! \pm m!$ durch q, nicht aber durch q^2 teilbar, also könnte (III) nicht bestehen.

Wenn also (III) unendlich viele Lösungen hätte, könnten wir Lösungen mit beliebig großem m finden. Für ein genügend großes m folgt aber aus der schärferen Form des Primzahlsatzes, daß es stets eine Primzahl q mit $\frac{m}{2} < q \leqq \frac{m}{2} + \frac{m}{12 \log m}$ gibt[20]). Also ergibt sich wie oben

(16) $$n \leqq m + \frac{m}{6 \log m}.$$

Aus (III) folgt nun

(17) $$m!\left(\frac{n!}{m!} \pm 1\right) = x^p.$$

$m!$ enthält jede Primzahl q mit $\frac{m}{2} < q \leqq m$ genau in der ersten Potenz. Wenn also (17) besteht, enthält $\frac{n!}{m!} \pm 1$ alle

[20]) Setzt man nämlich, wie üblich,

$$\vartheta(n) = \sum_{\substack{q \text{ Primzahl} \\ q \leqq n}} \log q,$$

so gilt bekanntlich

$$\vartheta(n) = n + O\left(\frac{n}{\log^2 n}\right),$$

also

$$\vartheta\left(\frac{m}{2} + \frac{m}{12 \log m}\right) - \vartheta\left(\frac{m}{2}\right) = \frac{m}{12 \log m} + O\left(\frac{m}{\log^2 m}\right) > 0$$

für hinreichend großes m.

diese Primfaktoren. Aus dem Primzahlsatze[21]) folgt, daß für hinreichend großes m das Produkt dieser Primzahlen größer als $2^{\frac{m}{2}}+1$ ist, folglich gilt

$$\frac{n!}{m!} > 2^{\frac{m}{2}}. \tag{18}$$

Aus $n \leqq m + \frac{m}{6 \log m} < 2m$ folgt aber

$$\frac{n!}{m!} = n(n-1)\ldots(m+1) < n^{n-m} < (2m)^{\frac{m}{6 \log m}} = 2^{\frac{m}{6 \log m}} e^{\frac{m}{6}},$$

was für hinreichend großes m offenbar mit (18) in Widerspruch steht. Es gilt daher

Satz 4. *Die unbestimmte Gleichung*

$$n! \pm m! = x^p$$

mit $n > m > 1$, $p > 1$ ist in großen Zahlen unmöglich, d. h. sie kann höchstens eine endliche Anzahl von Lösungen besitzen.

Die uns bekannten Lösungen der diophantischen Gleichung (III) sind

$$2!+2! = 2^2;\ 3!+2! = 2^3;\ 5!+4! = 12^2,\ 3!-2! = 2^2.$$

Wahrscheinlich sind diese Lösungen die einzigen.

Nach Abschluß der vorliegenden Arbeit ist es einem von uns (P. ERDŐS) gelungen, den Satz 4 auch elementar arithmetisch zu beweisen. Der Beweis ist aber nicht einfach und ist länger als der soeben gegebene.

Wir erfüllen eine angenehme Pflicht, indem wir Herrn L. KALMÁR für seine Ratschläge bestens danken.

(Eingegangen am 1. Februar 1937.)

[21]) Bekanntlich kann der Primzahlsatz auch in der Form ausgesprochen werden, daß das Produkt der Primzahlen zwischen $\frac{m}{2}$ und m gleich $e^{\frac{m}{2}+o(m)}$ ist.