Zur Arithmetik der Polynome.

Von TRYGVE NAGEL in Christiania (Norwegen).

§ 1. Eine Abschätzung über die Größe der Primteiler der Polynome.

In der Folge bedeutet $f(x)$ immer ein Polynom in x mit ganzzahligen (rationalen) Koeffizienten. Jede Primzahl p, für welche die Kongruenz

$$f(x) \equiv 0 \,(\mathrm{mod.}\, p)$$

Lösungen hat, wird ein Primteiler des Polynoms $f(x)$ genannt. Die Anzahl der inkongruenten Wurzeln dieser Kongruenz wird durch ν_p bezeichnet. Dann ist bekanntlich $\nu_p \leqq n$, wenn $f(x)$ primitiv und vom n^{ten} Grade ist.

In einer früheren Arbeit[1]) habe ich den folgenden Satz bewiesen: Wenn $f(x)$ mindestens eine irrationale Nullstelle hat, dann gibt es unter den Zahlen

$$f(1),\ f(2),\ f(3),\ \ldots\ldots\ldots,\ f(x)$$

wenigstens eine von Null verschiedene Zahl, die durch eine Primzahl $p > x\,(\log x)^{\varepsilon}$ teilbar ist, wo ε eine beliebige Größe < 1 ist, für alle $x > x_0$. Dieses Resultat soll hier bedeutend verschärft werden.

In der Folge wird von den folgenden Sätzen mehrmals Gebrauch gemacht[2]):

Hilfssatz I. Es sei $f(x)$ primitiv, vom n^{ten} Grade in x und ohne mehrfache Nullstellen. Dann hat die Kongruenz

$$f(x) \equiv 0 \,(\mathrm{mod.}\, p^{\alpha}),$$

1. wenn p nicht in der Diskriminante D von $f(x)$ aufgeht, genau ν_p inkongruente Wurzeln; 2. wenn p in D aufgeht, höchstens nD^2 inkongruente Wurzeln.

---

[1]) „Généralisation d'un théorème de TCHEBYCHEFF", Journal de Mathématiques, (8), t. IV (1921), p. 343—356. Literaturverzeichnis findet sich hier. Man vergleiche auch E. LANDAU, Handbuch der Lehre von der Verteilung der Primzahlen, Bd. 1, S. 559—564.

[2]) Die Beweise findet man in meiner oben erwähnten Arbeit. Den zweiten Hilfssatz beweise ich dort vom Primidealsatze ausgehend. In einer Arbeit des Herrn E. LANDAU, Über die zu einem algebraischen Zahlkörper gehörige Zetafunction und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf das Problem der Verteilung der Primideale, Journal für Mathematik, Bd. 125 (1903), S. 115, ist jedoch dieser Hilfssatz (die Formel (67) von LANDAU) unabhängig von der Theorie der ζ_n-Funktion bewiesen.

Hilfssatz II. Wenn $f(x)$ irreduzibel ist, gilt

$$\sum_{p}^{p \leqq x} \nu_p \frac{\log p}{p} = \log x + O(1),$$

wo die Summe über alle Primzahlen $\leqq x$ zu erstrecken ist.

Es sei nun gegeben das primitive irreduzible Polynom $f(x)$ vom Grade $n > 1$. Wir wollen zunächst die höchste Potenz p^N der Primzahl p bestimmen, die in dem Produkt

$$f(1) \cdot f(2) \cdot f(3) \cdots f(x) \tag{1}$$

aufgeht, wo x eine große ganze Zahl ist. Die Anzahl N_k der Zahlen in der Reihe

$$f(1), f(2), f(3), \ldots\ldots\ldots, f(x), \tag{2}$$

die durch p^k teilbar sind, ist offenbar gleich

$$N_k = \sum_{i=1}^{i=\lambda_k} \left[E\left(\frac{x - x_i^{(k)}}{p^k} \right) + 1 \right], \tag{3}$$

wo die λ_k Zahlen $x_1^{(k)}, x_2^{(k)}, \ldots\ldots\ldots, x_{\lambda_k}^{(k)}$ die sämtlichen positiven Wurzeln der Kongruenz

$$f(x) \equiv 0 \,(\mathrm{mod.}\, p^k)$$

bedeuten, die $\leqq p^k$ und zugleich $\leqq x$ sind. $E(a)$ bedeutet die größte ganze Zahl $\leqq a$. Es ist dann offenbar

$$N = N_1 + N_2 + N_3 + \ldots\ldots\ldots + N_l,$$

wo p^l die höchste Potenz von p ist, für welche die Kongruenz

$$f(x) \equiv 0 \,(\mathrm{mod.}\, p^l)$$

eine positive Wurzel hat, die $\leqq x$ ist.

Nun existieren zwei konstante Zahlen x_0 und c, so daß

$$c x^n > |f(x)| > |f(y)| \tag{4}$$

ist, für alle $x > x_0$, wenn $x > y > 0$ ist. Also ist sicher (für $x > x_0$)

$$p^l \leqq |f(x)| < c x^n$$

oder

$$l < \frac{\log c}{\log p} + n \frac{\log x}{\log p},$$

d. h.

$$l = \alpha \frac{\log x}{\log p}, \tag{5}$$

wo α unterhalb einer von x und p unabhängigen Grenze bleibt. Aus (3) erhalten wir:

$$N = \sum_{k=1}^{k=l} N_k = \sum_{i=1}^{i=\lambda_1} E\left(\frac{x+p-x_i^{(1)}}{p}\right) + \sum_{i=1}^{i=\lambda_2} E\left(\frac{x+p^2-x_i^{(2)}}{p^2}\right)$$
$$+ \ldots\ldots\ldots + \sum_{i=1}^{i=\lambda_l} E\left(\frac{x+p^l-x_i^{(l)}}{p^l}\right).$$

Nun ist

$$E\left(\frac{x+p^k-x_i^{(k)}}{p^k}\right) = \frac{x}{p^k} + \frac{p^k-x_i^{(k)}}{p^k} - \varepsilon_k = \frac{x}{p^k} + \theta_k,$$

wo $|\theta_k|<1$ ist. Folglich wird

$$N = x\frac{\lambda_1}{p} + x\frac{\lambda_2}{p^2} + \ldots\ldots\ldots + x\frac{\lambda_l}{p^l} + \sum_1^{\lambda_1}\theta_1 + \sum_1^{\lambda_2}\theta_2 + \ldots\ldots\ldots + \sum_1^{\lambda_l}\theta_l.$$

Nach dem Hilfssatze I ist aber

$$\lambda_k \leqq n D^2,$$

und folglich

$$\sum_1^{\lambda_1}|\theta_1| + \sum_1^{\lambda_2}|\theta_2| + \ldots\ldots\ldots + \sum_1^{\lambda_l}|\theta_l| < \lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l \leqq l n D^2$$

und

$$\frac{\lambda_2}{p^2} + \frac{\lambda_3}{p^3} + \ldots\ldots\ldots + \frac{\lambda_l}{p^l}$$
$$< \frac{n D^2}{p^2}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\ldots\ldots \text{in inf.}\right) = \frac{n D^2}{p(p-1)}.$$

Wegen (5) ergibt sich mithin

$$N = \lambda_1\frac{x}{p} + \beta_1\frac{\log x}{\log p} + \beta_2\frac{x}{p(p-1)}, \tag{6}$$

wo $|\beta_1|$ und $|\beta_2|$ unterhalb einer von x und p unabhängigen Grenze bleiben.

Wir bezeichnen von nun an alle Primteiler von dem Produkt (1), die $\leqq x$ sind, durch p, alle Primteiler aber, die $> x$ sind, durch q. x wählen wir so groß, daß alle Primteiler von (1), die in D aufgehen, sich unter den p befinden. Die Primzahlen p sind offenbar die sämtlichen Primteiler von dem Polynom $f(x)$, die $\leqq x$ sind. Für diese Primzahlen gilt $\lambda_1 = \nu_p$. Für die Primzahlen q folgt aus (3) einfach

$$N_k = \lambda_k$$

und also

$$N = \lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l. \tag{6'}$$

Hier ist offenbar für x hinreichend groß $l \leqq n$; denn wegen (4) ist

$$q^{n+1} > x^{n+1} > cx^n > |f(x)|$$

für alle $x > x_0$ und $> c$. Da die Primzahlen q nicht in D aufgehen, so gilt für sie $\lambda_k \leqq \nu_q \leqq n$.

Wegen (6) und (6′) erhalten wir die folgende Gleichung:

$$\sum_{k=1}^{k=x} \log|f(k)| = \sum_{p}^{p \leqq x} \left(\nu_p \frac{x}{p} + \beta_1 \frac{\log x}{\log p} + \beta_2 \frac{x}{p(p-1)}\right) \log p + \sum_{q} (\lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l) \log q.$$

Es ist offenbar

$$\sum_{p \leqq x} \beta_1 = O\left(\frac{x}{\log x}\right),$$

und weiter

$$\sum_{p \leqq x} \beta_2 \frac{\log p}{p(p-1)} = O(1),$$

weil die Reihe

$$\sum_{k=2}^{\infty} \frac{\log k}{k(k-1)}$$

konvergiert. Endlich ist nach dem Hilfssatze II:

$$\sum_{p}^{p \leqq x} \nu_p \frac{x \log p}{p} = x \log x + O(x).$$

Wir erhalten somit

$$\sum_{k=1}^{k=x} \log|f(k)| = x \log x + \sum_{q} (\lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l) \log q + O(x).$$

Da aber die Summe links offenbar von der Größenordnung

$$n x \log x + O(x)$$

ist, so ergibt sich schließlich

$$(7) \qquad \sum_{q} (\lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l) \log q = (n-1) x \log x + O(x),$$

wo die Summe über alle Primteiler q von (1), die $> x$ sind, zu erstrecken ist.

Diese Gleichung bleibt auch dann richtig, wenn man über alle $q > Cx$ summiert, wo C eine beliebige Konstante $\geqq 1$ ist. Denn es ist

$$\sum_{q > x}^{q \leqq Cx} (\lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l) \log q \leqq \sum_{q > x}^{q \leqq Cx} n l \cdot \log q \leqq n^2 \sum_{q < Cx} \log q = O(x).$$

Wir wählen nun $C^n \geqq c$, wo c die Konstante in (4) ist. Dann wird für alle $q > Cx$

$$q^n > C^n x^n \geqq c x^n > |f(x)| \geqq |f(y)|,$$

wenn $1 \leqq y \leqq x$ ist, für alle $x > x_0$. Folglich kann $f(y)$, $1 \leqq y \leqq x$, höchstens $n-1$ solche, verschiedene oder gleiche, Primzahlen $q > Cx$ enthalten; es ist somit $l \leqq n-1$.

Es sei nun A die Anzahl der Primzahlen q die $> Cx$ sind. Da

$$\lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_l \leqq nl \leqq n(n-1)$$

ist, und da wegen (4)

$$q \leqq |f(x)| < cx^n$$

ist, so folgt aus (7) (wenn hier die Summe über alle $q > Cx$ erstreckt ist)

$$n(n-1)(n\log x + \log c)A > (n-1)x\log x + O(x),$$

woraus

$$A > \frac{1}{n^2}x + O\left(\frac{x}{\log x}\right). \tag{8}$$

Andererseits ist, da $f(y)$ höchstens $n-1$ verschiedene Primteiler $q > Cx$ enthalten kann, offenbar

$$A < (n-1)x. \tag{9}$$

Für die (irreduziblen) quadratischen Polynome von der Form

$$ax^2 + b$$

gilt offenbar $\lambda_1 = 1$ für alle $q > 2x$. Denn ist ξ_0 die kleinste positive Wurzel der Kongruenz

$$a\xi^2 + b \equiv 0 \,(\mathrm{mod.}\, q),$$

also $0 < \xi_0 < \frac{1}{2}q$, so ist die nächste positive Wurzel gleich $q - \xi_0$ und folglich $> \frac{1}{2}q > x$. Für diese Polynome folgt mithin aus (7) die Formel

$$\sum_{q > Cx} \log q = x\log x + O(x), \tag{7'}$$

zunächst wenn $C \geqq 2$ ist; die Formel bleibt aber dann natürlich für jeden Wert von C richtig. Für die Anzahl der Primzahlen $q > Cx$ ergibt sich hieraus

$$A > \frac{1}{2}x + O\left(\frac{x}{\log x}\right). \tag{8'}$$

Es sei nun ε irgendeine positive Konstante < 1. Bezeichnet A' die Anzahl der Primzahlen $q > x(\log x)^\varepsilon$, so folgt offenbar aus (8)

$$A' > \frac{1}{n^2}x + O[x(\log x)^{\varepsilon - 1}], \tag{10}$$

und aus (8′) für die quadratischen Polynome ax^2+b sogar

$$A' > \frac{1}{2}x + O[x(\log x)^{\varepsilon-1}]. \tag{10′}$$

Denn die Anzahl aller Primzahlen $\leqq x(\log x)^{\varepsilon}$ ist ja gleich

$$O[x(\log x)^{\varepsilon-1}].$$

Aus (10) und (10′) folgt der Satz:

Es sei $f(x)$ eine ganze rationale, irreduzible Funktion n^{ten} Grades in x mit ganzzahligen Koeffizienten, $n>1$. Es sei weiter ε eine beliebige Größe <1, und δ eine beliebige Größe $<\frac{1}{n^2}$. Dann hat das Produkt

$$f(1)f(2)f(3)\cdots f(x) \tag{1}$$

mehr als δx verschiedene Primteiler die größer als $x(\log x)^{\varepsilon}$ sind, für alle $x>x_0$, wo x_0 von δ und ε abhängt. Für die quadratischen Polynome ax^2+b kann man hier sogar $\frac{1}{n^2}$ durch $\frac{1}{2}$ ersetzen[1]).

Bezeichnet $A(x;f)$ die Anzahl aller Primteiler des Produktes (1), so ergeben sich aus (8), (8′) und (9) die Ungleichungen

$$\frac{1}{n^2}x + O\left(\frac{x}{\log x}\right) < A(x;f) < (n-1)x + O\left(\frac{x}{\log x}\right),$$

wo für die quadratischen Polynome ax^2+b die Größe $\frac{1}{n^2}$ sogar durch $\frac{1}{2}$ ersetzt werden kann. Denn es ist ja

$$A(x;f) = A + O\left(\frac{x}{\log x}\right).$$

§ 2. Über potenzfreie Zahlen in einer arithmetischen Reihe höherer Ordnung.

Es sei gegeben die ganze rationale Funktion $f(x)$ n^{ten} Grades in x mit ganzen (rationalen) Koeffizienten. Es seien

$$p_1, p_2, p_3, \ldots\ldots\ldots, p_{m-1}, p_m, \ldots\ldots\ldots \tag{1}$$

die sämtlichen Primteiler des Polynoms $f(x)$ der Größe nach in einer Reihe angeordnet. Wenn s eine beliebig gegebene ganze Zahl $\geqq 2$ ist, so können wir immer ein m finden, so daß

[1]) Die Beschränkung, daß $f(x)$ primitiv sein soll, kann man hier selbstverständlich, wie auch in den Formeln von (7) ab, ohne weiteres weglassen.

$$\sum_{i=m}^{\infty} \frac{1}{p_i^s} < \frac{1}{n} \tag{2}$$

ist; denn die über *alle* Primzahlen ausgedehnte Reihe

$$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots\cdots\cdots$$

konvergiert ja.

Wir bezeichnen nun mit $I_s(x; f)$ die Anzahl der Zahlen in der Reihe

$$f(1),\ f(2),\ f(3),\ \ldots\ldots\ldots,\ f(x), \tag{3}$$

die durch keine s^{te} Potenz einer Primzahl teilbar sind.

Wir nehmen darauf an, 1. daß r der höchste Grad von allen in $f(x)$ aufgehenden irreduziblen Polynomen ist; 2. daß die Diskriminante D von $f(x)$ von Null verschieden ist; 3. daß $f(x)$ primitiv ist; 4. daß $f(x)$ keine s^{te} Potenz einer Primzahl als festen Teiler hat[1]). Weiter wählen wir in (2) m so groß, daß keine der Primzahlen p_i für $i \geqq m$ in D aufgeht.

Wegen der Voraussetzung 4. können wir eine ganze positive Zahl x_0 so finden, daß $f(x)$, wenn

$$x \equiv x_0 \,(\text{mod.}\, p_1^s p_2^s \cdots p_{m-1}^s)$$

ist, durch keine der Zahlen $p_1^s, p_2^s, \ldots\ldots\ldots, p_{m-1}^s$ teilbar ist. Wir setzen darauf

$$g(y) = f(x_0 + y p_1^s p_2^s \cdots p_{m-1}^s),$$

wo also $g(y)$ ein ganzzahliges Polynom n^{ten} Grades in y ist. Die Zahl r ist natürlich dieselbe für $g(y)$ wie für $f(x)$.

Es bezeichne nun $h_k(x)$ ein beliebiges ganzzahliges primitives irreduzibles Polynom, das in $g(x)$ aufgeht. Dann können wir (wegen der Voraussetzung 1) eine positive Konstante c finden, so daß für alle $h_k(x)$ und für alle $y > y_0$

$$|h_k(z)| \leqq |h_k(y)| < c y^r$$

ist, wenn $1 \leqq z \leqq y$ ist. Eine Primzahl p_i, wo $i \geqq m$ ist, kann nicht für denselben Wert von y gleichzeitig in $h_k(y)$ und $h_l(y)$, $k \neq l$, aufgehen. Denn jeder Primteiler der Resultante $R(h_k, h_l)$ geht bekanntlich in der Diskriminante D von $f(x)$ auf. Wenn $p_i > cy$ ist, ergibt sich

$$p_i^r > c^r y^r \geqq c y^r > |h_k(y)|.$$

---

[1]) $f(x)$ hat den festen Teiler d, wenn $f(x)$ für jeden ganzzahligen Wert von x durch d teilbar ist. Beispiel: $x^p - x$ hat den festen Teiler p, wenn p eine Primzahl ist.

$g(y)$ ist also für alle $y > y_0$ höchstens durch p_i^{r-1} teilbar, wenn $p_i > cy$ ist.

Nach dem Hilfssatz I in § 1 hat die Kongruenz

$$f(x) \equiv 0 \,(\mathrm{mod.}\, p_i^s), \tag{4}$$

wo $i \geqq m$ ist, höchstens n inkongruente Wurzeln. Nun hat aber die Kongruenz

$$g(y) = f(x_0 + y p_1^s \cdot p_2^s \cdots p_{m-1}^s) \equiv 0 \,(\mathrm{mod.}\, p_i^s)$$

genau so viele inkongruente Wurzeln wie (4), weil p_i nicht in $p_1 \cdot p_2 \cdots p_{m-1}$ aufgeht. Die Anzahl der Zahlen in der Reihe

$$g(1),\ g(2),\ g(3), \ldots\ldots\ldots,\ g(y), \tag{5}$$

die durch p_i^s teilbar sind, ist folglich höchstens gleich

$$n\left(\frac{y}{p_i^s} + 1\right). \tag{6}$$

Wir wollen hier zwei Fälle unterscheiden.

I. Es ist $r \geqq 2$, und $s = r$. Für die Anzahl der Zahlen in der Reihe (5), die durch keine r^{te} Potenz teilbar sind, folgt dann offenbar die Ungleichung

$$I_r(y; g) \geqq y - \sum_{p_i \geqq p_m}^{p_i \leqq cy} n\left(\frac{y}{p_i^r} + 1\right) \tag{7}$$

für alle $y > y_0$. Denn wir haben dann die Anzahl der eventuellen Zahlen n (5), die durch $p_i^r \cdot p_j^r$ teilbar sind, zweimal von allen y Zahlen abgezogen. Folglich

$$I_r(y; g) > y\left(1 - \sum_{i \geqq m}^{\infty} \frac{n}{p_i^r}\right) - n\pi(cy),$$

woraus wegen $\pi(x) = o(x)$

$$I_r(y; g) > K_0 y,$$

wo K_0 eine beliebige positive Größe kleiner als die nach (2) positive Zahl

$$C = 1 - \sum_{i \geqq m}^{\infty} \frac{n}{p_i^r}$$

ist. Da für $x = x_0 + y p_1^r \cdot p_2^r \cdots p_{m-1}^r = x_0 + yP$

$$I_r\left(\frac{x - x_0}{P}; f\right) \geqq I_r(y; g)$$

ist, folgt schließlich

$$I_r(x; f) > Kx, \tag{8}$$

wo K eine beliebige positive Größe kleiner als $\frac{C}{P}$ ist, für alle $x > x_0$. Speziell ergibt sich also hieraus:

Unendlich viele Zahlen in der Reihe

$$f(1),\ f(2),\ f(3), \ldots\ldots\ldots \text{ in inf.}$$

sind durch keine r^{te} Potenz einer Primzahl teilbar.

Beispiel:

Es sei $f(x) = x^2+1$. Die Primteiler von f sind dann entweder 2 oder alle Primzahlen von der Form $4t+1$. Wir erhalten hier, wie sogleich zu ersehen ist, statt (7) die etwas schärfere Ungleichung

$$I_2(x; x^2+1) \geqq x - \sum_{p_i > 2}^{p_i \leqq x} \left(\frac{2x}{p_i^2}+1\right),$$

wo die Summe über alle Primzahlen $p_i \leqq x$ von der Form $4t+1$ zu erstrecken ist. Denn ist $p_i > x$, so ist ja $p_i^2 \geqq (x+1)^2 > x^2+1$. Es ist hier nicht notwendig, den Umweg über die Funktion $g(y)$ zu gehen. Denn der einzige Diskriminantenteiler, die Primzahl 2, geht nur zur ersten Potenz in x^2+1 auf; und es ist zugleich

$$\frac{1}{5^2}+\frac{1}{13^2}+\frac{1}{17^2}+\ldots\ldots < \frac{1}{4^2}+\frac{1}{8^2}+\frac{1}{12^2}+\ldots\ldots = \frac{1}{16}\cdot\frac{\pi^2}{6} < \frac{5}{48}.$$

Folglich

$$I_2(x; x^2+1) > \frac{19}{24}x - \pi_2(x),$$

wo $\pi_2(x)$ die Anzahl aller Primzahlen von der Form $4t+1 \leqq x$ bedeutet. Bezeichnet nun $B(z; 3, 5, 7)$ die Anzahl der Zahlen in der Reihe

$$5, 9, 13, 17, \ldots\ldots\ldots, 4z+1,$$

die durch keine der Zahlen 3, 5 oder 7 teilbar sind, so ist offenbar

$$\pi_2(4z+1) \leqq 1 + B(z; 3, 5, 7).$$

Da nun

$$B(z; 3, 5, 7) < z - \frac{1}{3}z - \frac{1}{5}z - \frac{1}{7}z + \frac{1}{15}z + \frac{1}{21}z + \frac{1}{35}z - \frac{1}{105}z + 4$$

$$= 4 + z\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 4 + \frac{16}{35}z$$

ist, so folgt

$$\pi_2(x) < \frac{4}{35}x + 5$$

oder

$$I_2(x; x^2+1) > \frac{569}{840}x - 5 > \frac{2}{3}x, \tag{9}$$

zunächst für alle $x > 466$. Eine Aufzählung der durch Primzahlquadrate teilbaren Zahlen x^2+1 für $x \leqq 466$ zeigt, daß diese Ungleichung für alle positiven x gültig ist. Man kann dies auch so aussprechen:

Die Anzahl der quadratfreien Zahlen $D \leqq z$, für welche die Pellsche Gleichung

$$x^2 - Dy^2 = -1$$

die Fundamentallösung $y_1 = 1$ hat, ist größer als $\frac{2}{3}\sqrt{z}$. (Andererseits ist diese Anzahl selbstverständlich kleiner als $\sqrt{z}$.)

II. Es ist $r = 1$ und $s = 2$. Für die Anzahl der quadratfreien Zahlen in der Reihe (5) erhalten wir hier die Ungleichung

$$I_2(y; g) \geqq y - \sum_{p_i \geqq p_m}^{p_i \leqq \sqrt{cy}} n\left(\frac{y}{p_i^2} + 1\right). \tag{10}$$

Denn für $p_i > \sqrt{cy}$, wird

$$p_i^2 > cy > |h_k(y)|,$$

für alle $y > y_0$. Soll $g(y)$, für $y > y_0$, durch p_i^2 teilbar sein, muß also $p_i \leqq \sqrt{cy}$ sein. Setzen wir, wie früher, $P = p_1^2 \cdot p_2^2 \cdots p_{m-1}^2$ und

$$C = 1 - \sum_{i \geqq m}^{\infty} \frac{n}{p_i^2},$$

so ergibt sich schließlich

$$I_2(x; f) > Kx, \tag{11}$$

wo K eine beliebige positive Größe kleiner als $\frac{C}{P}$ ist, für alle $x > x_0$. Speziell ergibt sich z. B. der folgende Satz:

Es gibt unendlich viele positive ganzzahlige Werte von x, für welche die Zahlen

$$a_1 x + b_1, \quad a_2 x + b_2, \quad a_3 x + b_3$$

sämtlich quadratfrei sind, wenn keine der Zahlen (a_i, b_i) durch ein Primzahlquadrat teilbar sind.

Denn ein primitives Polynom von niedrigerem Grade als dem 4^{ten} kann kein Primzahlquadrat als festen Teiler haben.

Beispiel:

Es sei $f(x) = 4x^2 - 1$. Wir erhalten hier die Ungleichung

$$I_2(x; 4x^2-1) \geqq x - \sum_{p_i \geqq 3}^{p_i \leqq \sqrt{2x+1}} \left(\frac{2x}{p_i^2} + 1\right),$$

wo die Summe über alle ungeraden Primzahlen $\leqq \sqrt{2x+1}$ zu erstrecken ist. Es ist hier nicht notwendig, den Umweg über die Funktion $g(y)$

zu gehen. Denn der einzige Diskriminantenteiler, die Primzahl 2, geht nicht in $4x^2-1$ auf; und es ist zugleich

$$\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{11^2}+\ldots\ldots\ldots<\frac{8}{9}\sum_{k=1}^{\infty}\frac{1}{(2k+1)^2}=\frac{\pi^2}{9}-\frac{8}{9}<\frac{2}{9}.$$

Folglich

$$I_2(x;\,4x^2-1)>\frac{5}{9}x-\pi(\sqrt{2x+1})$$

oder da für alle $x>162$

$$\pi(\sqrt{2x+1})<\frac{1}{2}\sqrt{2x+1}<\frac{1}{18}x,$$

so ergibt sich schließlich

$$I_2(x;\,4x^2-1)>\frac{1}{2}x. \tag{12}$$

Eine kurze Rechnung zeigt, daß diese Ungleichung auch für alle positiven $x\leqq 162$ gültig ist. Man kann dies auch so aussprechen:

Die Anzahl der quadratfreien Zahlen $D\leqq z$, für welche die Pellsche Gleichung

$$x^2-Dy^2=1$$

die Fundamentallösung $y_1=1$ hat, ist größer als $\frac{1}{4}\sqrt{z+1}$.

Anmerkung:

Man beweist auch leicht den allgemeineren Satz:

Es sei y_1 eine beliebige positive ganze Zahl. Dann ist die Anzahl der quadratfreien Zahlen $D\leqq z$, für welche die Pellsche Gleichung

$$x^2-Dy^2=1$$

die Fundamentallösung $y=y_1$ hat, größer als $k\sqrt{z}$, wo k eine von y_1 abhängige positive Konstante ist.

Diesen Satz haben wir also für $y_1=1$ schon bewiesen. Wir wollen zunächst den folgenden Hilfssatz beweisen:

Gilt für ein Paar von positiven Lösungen $x=x_1$, $y=y_1$ der Pellschen Gleichung

$$x^2-Dy^2=1$$

die Ungleichung

$$x_1>\frac{1}{2}y_1^2-1, \tag{13}$$

dann sind x_1 und y_1 die Fundamentallösungen der Gleichung[1]).

Da die Fundamentallösungen die kleinsten (positiven) Lösungen sind, so ist der Satz evident für $y_1=1$. Wären etwa $x=\xi$ und $y=\eta$ die Fundamentallösungen und $1\leqq\eta<y_1$, so erhielten wir

[1]) Daß diese Ungleichung nicht allgemein für die Fundamentallösungen gilt, lehrt das Beispiel $D=13$ mit $x_1=649$ und $y_1=180$, also $\frac{1}{2}y_1^2-1=16199>x_1$.

$$D = \frac{\xi^2 - 1}{\eta^2} = \frac{x_1^2 - 1}{y_1^2}$$

oder

$$\xi^2 y_1^2 - x_1^2 \eta^2 = y_1^2 - \eta^2 = d > 0,$$

woraus

$$\xi y_1 + x_1 \eta = d_1, \quad \xi y_1 - x_1 \eta = d_2,$$

wo $d_1 d_2 = d$ ist; folglich

$$x_1 = \frac{d_1 - d_2}{2\eta} \leqq \frac{d-1}{2\eta} = \frac{y_1^2 - \eta^2 - 1}{2\eta} \leqq \frac{1}{2} y_1^2 - 1,$$

in Widerspruch zu (13). Also ist der Hilfssatz bewiesen.

Folglich haben alle Zahlen

$$D = \frac{1}{y_1^2}[(1 + u y_1^2)^2 - 1] = u(u y_1^2 + 2), \tag{14}$$

wo u eine beliebige positive ganze Zahl ist, die Eigenschaft, daß die Pellsche Gleichung

$$x^2 - D y^2 = 1$$

die Fundamentallösung $y = y_1$ hat. Wir haben aber soeben gesehen, daß die Anzahl der Zahlen (14), die quadratfrei und $\leqq z$ sind, größer als $k\sqrt{z}$ ist, wo die positive Zahl k nur von y_1 abhängt. Unser Satz ist damit bewiesen. Ja, man sieht leicht ein, daß der Satz sogar auch dann gilt, wenn man verlangt, daß D gewissen Kongruenzbedingungen genügen soll (z. B., daß D durch 5 teilbar sein soll, usf.). Ganz analog beweist man den folgenden Satz:

Es sei y_1 eine beliebige positive ganze Zahl, deren Primfaktoren nur Primzahlen von der Form $4t+1$ sind. Dann ist die Anzahl der quadratfreien Zahlen $\leqq z$, für welche die Pellsche Gleichung

$$x^2 - D y^2 = -1$$

die Fundamentallösung $y = y_1$ hat, größer als $k\sqrt{z}$, wo k eine von y_1 abhängige positive Konstante ist.

Entsprechende Resultate folgen natürlich für die Grundeinheiten in quadratischen Zahlkörpern.

§ 3. Eine Bemerkung über die Anzahl der Primzahlen in einer arithmetischen Reihe höherer Ordnung.

Soll die Reihe

$$f(1), f(2), f(3), \ldots\ldots \text{in inf.}$$

unendlich viele Primzahlen enthalten, muß das Polynom $f(x)$ natürlich irreduzibel und ohne feste Teiler sein. Es sei nun gegeben das

irreduzible Polynom $f(x)$ n^{ten} Grades in x, das keinen festen Teiler hat. Wir wollen zunächst den folgenden Hilfssatz beweisen: Wenn ν_p (wie früher in § 1) die Anzahl der inkongruenten Wurzeln der Kongruenz

$$f(x) \equiv 0 \pmod{p}$$

bedeutet, so ist

$$\lim_{x\to\infty} \prod_{p\leqq x} \left(1-\frac{\nu_p}{p}\right) = 0, \tag{1}$$

wo das Produkt über alle Primzahlen $p \leqq x$ zu erstrecken ist.

Es genügt, den Satz für solche Polynome zu beweisen, für welche der Koeffizient von x^n gleich 1 ist. Denn ist dieser Koeffizient a_0, setzen wir

$$a_0^{n-1} f(x) = g(z),$$

wo $z = a_0 x$ ist; die Anzahl der inkongruenten Wurzeln der Kongruenz

$$f(x) \equiv 0 \pmod{p},$$

wo p eine Primzahl ist, ist aber genau gleich der Anzahl der inkongruenten Wurzeln der Kongruenz

$$g(z) \equiv 0 \pmod{p},$$

wenn p nur nicht in a_0 aufgeht.

Es sei nun $K(\alpha)$ der durch die Wurzel α von $f(x) = 0$ erzeugte Körper n^{ten} Grades. Dann gilt bekanntlich[1])

$$\lim_{x\to\infty} \prod_{N(\mathfrak{p})\leqq x} \left(1-\frac{1}{N(\mathfrak{p})}\right) = 0, \tag{2}$$

wo das Produkt über alle Primideale $\mathfrak{p}$ in $K(\alpha)$, deren Norm $N(\mathfrak{p}) \leqq x$ ist, zu erstrecken ist.

Es sei nun $\nu_p^{(r)}$ die Anzahl der (verschiedenen) Primideale r^{ten} Grades, die im Hauptideal $[p]$ aufgehen, wo p eine (rationale) Primzahl ist. Dann ist

$$\prod_{N(\mathfrak{p})\leqq x} \left(1-\frac{1}{N(\mathfrak{p})}\right)$$
$$= \prod_{p\leqq x} \left(1-\frac{1}{p}\right)^{\nu_p^{(1)}} \prod_{p^2\leqq x} \left(1-\frac{1}{p^2}\right)^{\nu_p^{(2)}} \cdots \prod_{p^n\leqq x} \left(1-\frac{1}{p^n}\right)^{\nu_p^{(n)}},$$

wo die Produkte über alle Primzahlen $p \leqq x$ bzw. $\leqq x^{\frac{1}{2}}, \ldots\ldots$ bzw. $\leqq x^{\frac{1}{n}}$ zu erstrecken sind. Nun konvergiert aber das Produkt

[1]) Siehe z. B. E. LANDAU, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale (Leipzig 1918), Teil 2.

$$\prod_{p}^{\infty}\left(1-\frac{1}{p^r}\right)^{\nu_p^{(r)}}$$

für $r \geqq 2$. Denn es ist

$$\left(1-\frac{1}{p^r}\right)^{\nu_p^{(r)}} \geqq \left(1-\frac{1}{p^r}\right)^{n},$$

und die über alle Primzahlen p erstreckte Summe

$$\sum_{p}^{\infty}\frac{1}{p^r}$$

konvergiert für $r \geqq 2$. Wegen (2) ist somit

$$\lim_{x\to\infty}\prod_{p\leqq x}\left(1-\frac{1}{p}\right)^{\nu_p^{(1)}} = 0.$$

Weiter ist $\nu_p^{(1)} = \nu_p$ für alle Primzahlen, die endlich vielen Primteiler des Index der ganzen Zahl α eventuell ausgenommen[1]). Da endlich

$$\left(1-\frac{1}{p}\right)^{\nu_p} \geqq \left(1-\frac{\nu_p}{p}\right) > 0$$

ist, so ist unser Hilfssatz bewiesen.

Es seien nun

$$p_1, p_2, p_3, \ldots\ldots\ldots, p_m, \ldots\ldots\ldots \tag{3}$$

die sämtlichen Primteiler von $f(x)$ der Größe nach angeordnet.

Es sei gegeben die positive Zahl δ. Dann existiert ein m, so daß

$$\prod_{p_1\leqq p\leqq p_m}\left(1-\frac{\nu_p}{p}\right) < \frac{1}{2}\delta \tag{4}$$

ist. Indem wir die Anzahl der Primzahlen in der Reihe

$$f(1), f(2), f(3), \ldots\ldots\ldots, f(x) \tag{5}$$

durch $\pi(x; f)$ bezeichnen, wollen wir den folgenden Satz beweisen:

$$\pi(x; f) = o(x). \tag{6}$$

Der Beweis ist dem Beweis für die gewöhnliche Primzahlfunktion $\pi(x)$ ganz analog[2]).

[1]) DEDEKIND, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen, Abh. der K. Ges. der Wiss. zu Göttingen, 1878.

[2]) Siehe z. B. E. LANDAU, Handbuch der Lehre von der Verteilung der Primzahlen, Bd. 1, S. 69—71.

Auch für den Fall $f(x) = x^2 + 1$ ist der Satz früher bewiesen[1]). Es bezeichne $B(x; p_1, p_2, \ldots\ldots, p_m)$ die Anzahl der Zahlen in der Reihe (5), die durch keine der m ersten Primzahlen $p_1, p_2, \ldots\ldots, p_m$ der Reihe (3) teilbar sind. Dann ist offenbar

$$\pi(x; f) \leqq m + B(x; p_1, p_2, \ldots\ldots, p_m). \tag{7}$$

Es sei ξ eine Größe, so daß

$$\xi > p_1 p_2 \cdots p_m \tag{8}$$

und zugleich

$$\frac{\delta}{2}\xi > (1+n)^m + m - 1. \tag{9}$$

Dann betrachten wir nur solche x, die $\geqq \xi$ sind. Es sei nun

$$D = p_i p_j \cdots p_l$$

ein Produkt aus verschiedenen der Primzahlen $p_1, p_2, \ldots\ldots, p_m$. Dann ist die Anzahl der Zahlen in der Reihe (5) die durch D teilbar sind, gegeben durch[2])

$$E\left(\frac{x - x_1^{(D)}}{D}\right) + 1 + E\left(\frac{x - x_2^{(D)}}{D}\right) + 1 + \ldots\ldots + E\left(\frac{x - x_N^{(D)}}{D}\right) + 1,$$

wo $x_1^{(D)}, x_2^{(D)}, \ldots\ldots, x_N^{(D)}$ die N positiven Wurzeln der Kongruenz

$$f(x) \equiv 0 (\mathrm{mod.}\, D)$$

sind, die $\leqq D$ und zugleich $\leqq x$ sind. Da aber $D \leqq p_1 p_2 \cdots p_m < \xi \leqq x$ ist, folgt, daß

$$N = \nu_{p_i} \cdot \nu_{p_j} \cdots \nu_{p_l}$$

ist. Es ergibt sich somit nach bekannten Überlegungen

$$B(x; p_1, p_2, \ldots\ldots, p_m) = x + \sum_{D>1} \mu(D) \sum_{k=1}^{k=N} E\left(\frac{x - x_k^{(D)}}{D} + 1\right),$$

wo man über alle Teiler > 1 des Produktes $p_1 \cdot p_2 \cdots p_m$ zu summieren hat. Setze ich hier statt dem Gliede

$$E\left(\frac{x - x_k^{(D)}}{D} + 1\right)$$

---

[1]) Siehe VIGGO BRUN, Om fordelingen av primtallene i forskjellige talklasser, Nyt Tidsskrift for Matematik, Bd. XXVII (Kopenhagen 1916).

[2]) $E(a)$ bedeutet die größte ganze Zahl $\leqq a$.

die Zahl

$$\frac{x}{D},$$

so begehe ich höchstens einen Fehler von der Größe 1 $\left(\text{denn } 0 \leqq 1 - \frac{x_k^{(D)}}{D} < 1\right)$, also für alle Glieder einen Fehler kleiner als

$$\sum_{D>1} \mu^2(D) \cdot N = \sum \nu_{p_i} + \sum \nu_{p_i} \cdot \nu_{p_j} + \ldots\ldots\ldots + \nu_{p_1} \cdot \nu_{p_2} \cdots \nu_{p_m}$$
$$\leqq \binom{m}{1} n + \binom{m}{2} n^2 + \ldots\ldots\ldots + \binom{m}{m} n^m.$$

Aus (7) folgt mithin

$$\pi(x; f) < (1+n)^m + m - 1 + x + \sum_{D>1} \mu(D) \frac{x}{D} \cdot N.$$

Nun ist nach (4)

$$1 + \sum_{D>1} \mu(D) \frac{N}{D} = \prod_{p \leqq p_m} \left(1 - \frac{\nu_p}{p}\right) < \frac{1}{2} \delta.$$

Wegen (8) und (9) folgt also

$$\pi(x; f) < \frac{1}{2} \delta \xi + \frac{1}{2} \delta x \leqq \delta x$$

oder

$$\lim_{x \to \infty} \frac{\pi(x; f)}{x} = 0,$$

w. z. b. w.

Hamburg, Mathematisches Seminar, Dezember 1921.