ÜBER DEN GRÖSSTEN PRIMTEILER DER POLYNOME X^2+1

VON

KURT MAHLER

OSLO
I KOMMISSION HOS MORTEN JOHANSEN
1933

ÜBER DEN GRÖSSTEN PRIMTEILER DER POLYNOME x^2+1.

VON

KURT MAHLER

IN KREFELD

Das Ziel der folgenden Note ist der Beweis zweier einfachen Sätze über die grösste Primzahl, die in x^2-1 und x^2+1 aufgeht:

»*Ist $x \geq 2$ eine natürliche Zahl und $P_1(x)$ die grösste Primzahl, die in x^2-1 aufgeht, so ist*

$$\lim_{x \to \infty} \frac{P_1(x)}{\log \log x} \geq 1.«$$

»*Ist x eine natürliche Zahl und $P_2(x)$ die grösste Primzahl, die in x^2+1 aufgeht, so ist*

$$\lim_{x \to \infty} \frac{P_2(x)}{\log \log x} \geq 2.«$$

Ich wurde zu dem Beweis dieser Sätze angeregt durch die Lektüre der bekannten Arbeiten von Carl Størmer, in denen gezeigt wird, wie man in endlichvielen Schritten alle natürlichen Zahlen x bestimmen kann, für die in x^2-1 oder x^2+1 nur endlichviele gegebenen Primzahlen aufgehen. Durch Hinzunahme einiger bekannten Abschätzungen über die Pellsche Gleichung kommt man mittels seiner Methode leicht zu den angegebenen Ergebnissen.

Es wäre von Interesse, entsprechende Abschätzungen für beliebige Polynome herzuleiten; wenn diese mindestens zwei verschiedene Nullstellen haben, so weiss man nach Polya und Siegel bisher nur, dass mit wachsendem x die grösste im Polynom aufgehende Primzahl über alle Grenzen wächst, weiss aber nicht, wie schnell dies geschieht.

1) Satz 1: *Sei D eine natürliche Zahl, die kein Quadrat ist, T, U die kleinste Lösung der Pellschen Gleichung*

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

in natürlichen Zahlen $x = T$, $y = U$. Dann besteht die Ungleichung

$$\log(T + U\sqrt{D}) \leq 2\sqrt{D}\log(8D).$$

Beweis: Bedeutet h die Klassenanzahl der eigentlich primitiven indefiniten quadratischen Binärformen der Determinante D, so besteht bekanntlich nach Gauss und Dirichlet die Gleichung[1])

$$h\log(T + U\sqrt{D}) = 2\sqrt{D}\sum_{n=1}^{\infty} X(n)\cdot\frac{1}{n};$$

hierbei ist $X(n)$ ein gewisser Charakter mod $8D$, auf dessen genauen Wert es für die folgenden Zwecke nicht ankommt; demnach gilt

$$|X(n)| \leq 1,\ X(n) = X(n')\ \text{für}\ n \equiv n' \pmod{8D},\ \sum_{n=1}^{8D} X(n) = 0.$$

Beachtet man, dass h als nichtverschwindende Anzahl mindestens gleich Eins ist, so geht die Gleichung für $\log(T + U\sqrt{D})$ über in die Ungleichung

$$\log(T + U\sqrt{D}) \leq 2\sqrt{D}\sum_{n=1}^{\infty} X(n)\cdot\frac{1}{n}.$$

Die unendliche Summe rechts lässt sich in üblicher Weise mittels der Integralformel

$$\int_0^1 z^{n-1}dz = \frac{1}{n}$$

summieren; alsdann ergibt sich

$$\log(T + U\sqrt{D}) \leq 2\sqrt{D}\int_0^1 \frac{\sum_{n=1}^{8D} X(n)z^{n-1}}{1 - z^{8D}}\,dz.$$

Der Integrand

$$\Phi(z) = \frac{\sum_{n=1}^{8D} X(n)z^{n-1}}{1 - z^{8D}}$$

ist eine rationale Funktion, deren Nenner genau durch die erste Potenz von $1 - z$ teilbar ist. Wegen

$$\sum_{n=1}^{8D} X(n) = 0$$

[1]) Vergleiche etwa: P. Bachmann, Analytische Zahlentheorie (Leipzig 1894), 6. Abschnitt, Formel (22).

muss sich auch der Zähler durch $1-z$ teilen lassen; führt man diese Division wirklich durch, so erhält man

$$\frac{1}{1-z}\sum_{n=1}^{8D} X(n)z^{n-1} = X(1)+(X(1)+X(2))z+\cdots+(X(1)+X(2)+\cdots+X(8D-1))z^{8D-2},$$

wegen

$$|X(n)| \leq 1$$

demnach erst recht

$$\left|\frac{1}{1-z}\sum_{n=1}^{8D} X(n)z^{n-1}\right| \leq \sum_{n=1}^{8D-1} nz^{n-1}$$

und damit

$$|\Phi(z)| \leq \frac{d\log \sum_{n=0}^{8D-1} z^n}{dz} = \Psi(z).$$

Man kann die Integration über diese Majorante ohne weiteres durchführen; sie liefert

$$\log(T+U\sqrt{D}) \leq 2\sqrt{D}\int_0^1 \Phi(z)dz \leq 2\sqrt{D}\int_0^1 \Psi(z)dz = 2\sqrt{D}\log(8D),$$

und das sollte bewiesen werden.

Satz 2: *Sei D eine natürliche Zahl, die kein Quadrat ist, T', U' die kleinste Lösung der Gleichung*

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

in natürlichen Zahlen $x = T'$, $y = U'$, falls diese lösbar ist. Dann gilt

$$\log(T'+U'\sqrt{D}) < \sqrt{D}\log(8D).$$

Beweis: Bekanntlich besteht die Beziehung

$$T+U\sqrt{D} = (T'+U'\sqrt{D})^2,$$

so dass die Behauptung aus Satz 1 folgt.

2) Satz 3: *Sei ε eine beliebig kleine positive Konstante, z eine positive Zahl, die oberhalb einer von ε abhängigen Schranke liegt. Dann ist das Produkt aller Primzahlen $p \leq z$ höchstens gleich*

$$e^{(1+\frac{\varepsilon}{2})z}.$$

Satz 4: *Sei ε eine beliebig kleine positive Konstante, z eine positive Zahl, die oberhalb einer von ε abhängigen Schranke liegt, Dann ist das Produkt aller Primzahlen $p \leq z$, die als Teiler des Polynoms x^2+1 auftreten können, höchstens gleich*

$$e^{\frac{1}{2}(1+\frac{\varepsilon}{2})z}.$$

Beweis: Satz 3 folgt ohne weiteres aus dem Primzahlsatz[1]). Um Satz 4 zu beweisen, beachte man, dass die Zahlen der Form x^2+1 nur durch die Primzahl 2 und die Primzahlen der Form $4h+1$ teilbar sind; die Behauptung folgt also, wenn man das Analogon des Primzahlsatzes für diese spezielle arithmetische Reihe anwendet[2]).

3) Satz 5: *Sind $p_1, p_2, \ldots, p_t$ endlichviele verschiedene Primzahlen, so ist jede natürliche Zahl x, für die x^2-1 höchstens durch diese Primzahlen teilbar ist, enthalten unter den Fundamentallösungen $x = T$ der Pellschen Gleichungen*

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

dabei durchläuft D die sämtlichen natürlichen Zahlen

$$D = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t},$$

die keine Quadrate sind und deren Exponenten 0 oder 1 oder 2 sind.

Satz 6: *Sind $p_1, p_2, \cdots, p_t$ endlichviele verschiedene Primzahlen, so ist jede natürliche Zahl x, für die x^2+1 höchstens durch diese Primzahlen teilbar ist, enthalten unter den Fundamentallösungen $x = T'$ der Gleichungen*

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

dabei durchläuft D die sämtlichen natürlichen Zahlen

$$D = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t},$$

die keine Quadrate sind und deren Exponenten 0 oder 1 oder 2 sind.

Die beiden Sätze 5 und 6 stammen von Carl Størmer; wegen des Beweises sei auf seine Abhandlung verwiesen[3]).

4) Die Sätze 1—6 erlauben, eine positive Schranke $Z_1(z)$, bzw. $Z_2(z)$ anzugeben, sodass für jede natürliche Zahl $x \geq Z_1(z)$ das Polynom x^2-1 und für jede natürliche Zahl $x \geq Z_2(z)$ das Polynom x^2+1 durch eine Primzahl grösser als z teilbar ist.

Es werde erstens Satz 5 angewandt, indem dort für $p_1, p_2, \cdots, p_t$

---

[1]) Vergleiche etwa: E. Landau, Vorlesungen über Zahlentheorie II (Leipzig 1927), s. 47, Satz 402. Man muss $k=1$, $l=0$ nehmen.

[2]) Siehe [1]). Man muss $k=4$, $l=1$ nehmen.

[3]) Siehe z. B. die Abhandlung: Carl Størmer, Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = +1$ et leurs applications, Videnskapsselskabets Skrifter, I. Mathem.-naturvid. Klasse, (1897), No. 2.

die Gesamtheit aller Primzahlen eingesetzt wird, die z nicht überschreiten. Dann ist

$$D \leqq p_1^2 p_2^2 \cdots p_l^2$$

und nach Satz 3 für hinreichend grosses z

$$D \leqq e^{2\left(1+\frac{\varepsilon}{2}\right)z}.$$

Nach Satz 1 genügt demnach die Fundamentallösung T, U der mit D gebildeten Pellschen Gleichung

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

für hinreichend grosses z der Ungleichung

$$\log(T+U\sqrt{D}) < 2e^{\left(1+\frac{\varepsilon}{2}\right)z}\left[2\left(1+\frac{\varepsilon}{2}\right)z + \log 8\right]$$

und also ist erst recht für $z \geqq z_1(\varepsilon)$

$$T < T+U\sqrt{D} \leqq e^{2e^{(1+\varepsilon)z}}.$$

Damit haben wir folgendes Ergebnis bewiesen:

1. Ergebnis: *Ist ε positiv und beliebig klein, ferner die positive Zahl z oberhalb einer von ε abhängigen Schranke, so geht für jede natürliche Zahl x mit*

$$x \geqq e^{2e^{(1+\varepsilon)z}}$$

eine Primzahl grösser als z auf in dem Polynom x^2-1.

Es werde zweitens Satz 6 angewandt, indem dort für $p_1, p_2, \cdots, p_l$ die Gesamtheit aller Primzahlen eingesetzt wird, die z nicht überschreiten und die als Teiler des Polynoms x^2+1 auftreten können, d. h. gleich 2 oder von der Form $4h+1$ sind. Dann ist

$$D \leqq p_1^2 p_2^2 \cdots p_l^2$$

und nach Satz 4 für hinreichend grosses z

$$D \leqq e^{\left(1+\frac{\varepsilon}{2}\right)z}.$$

Nach Satz 2 genügt demnach die Fundamentallösung T', U' der mit D gebildeten Gleichung

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

für hinreichend grosses z der Ungleichung

$$\log(T'+U'\sqrt{D}) \leqq e^{\frac{1}{2}\left(1+\frac{\varepsilon}{2}\right)z}\left[\left(1+\frac{\varepsilon}{2}\right)z + \log 8\right]$$

und also ist erst recht für $z \geqq z_2(\varepsilon)$

$$T' < T'+U'\sqrt{D} \leqq e^{e^{\frac{1}{2}(1+\varepsilon)z}}.$$

Damit ist bewiesen:

2. Ergebnis: *Ist ε positiv und beliebig klein, ferner die positive Zahl z oberhalb einer von ε abhängigen Schranke, so geht für jede natürliche Zahl x mit*

$$x \geq e^{e^{\frac{1}{2}(1+\varepsilon)z}}$$

in dem Polynom x^2+1 eine Primzahl grösser als z auf.

5) Aus dem 1. und 2. Ergebnis folgen die in der Einleitung genannten Sätze, wenn man nach z auflöst und beachtet, dass ε beliebig klein sein darf.

Es scheint nicht leicht zu sein, ein entsprechendes Ergebnis für beliebige Polynome abzuleiten. Jedoch ist es möglich, durch Variablenänderung beliebig viele andere Polynome herzustellen, für die sich der in ihnen aufgehende grösste Primteiler gleichfalls nach unten abschätzen lässt. Hiervon seien als besonders interessant erwähnt die Polynome

$$x(x+1),\ x(x+2).$$

Krefeld, 10. Juli 1933.