SS 2017 Dr. Michael H. Mertens

Elementare Zahlentheorie

Übungsblatt 9 Lösung

Aufgabe 2. Zeigen Sie, dass es unendlich viele Primzahlen der Form $15k+4$ mit $k \in \mathbb{N}$ gibt. Betrachten Sie dazu das Polynom

$$f(x) = x^4 - x^3 + 2x^2 + x + 1.$$

Folgen Sie den folgenden Schritten, um die genannte Behauptung zu zeigen.

(a) Ist $p \in \mathbb{P}$, $p \nmid 30$ ein Primteiler von $f(n)$, $n \in \mathbb{Z}$, so gilt

$$\left(\frac{p}{3}\right)\left(\frac{p}{5}\right) = 1,$$

also $p \equiv 1, 2, 4, 8 \pmod{15}$.

Hinweis: Verwenden Sie $f(x) = (x^2 - x/2 - 1)^2 + 15x^2/4$ und folgern Sie, dass -15 ein quadratischer Rest modulo p sein muss.

(b) Zeigen Sie, dass für p wie in (a)

$$\left(\frac{-3}{p}\right) = 1,$$

also $p \equiv 1, 7 \pmod{12}$ gilt.

Hinweis: Verwenden Sie $f(x) = (-x^2 + x/2 - 1/2)^2 + 3(x+1)^2/4$.

(c) Zeigen Sie, dass jedes p wie in (a) die Kongruenz $p \equiv \pm 1 \pmod{5}$ erfüllt.

Hinweis: Verwenden Sie $f(x) = (-x^2 + x/2 - 3/2)^2 - 5(x-1)^2/4$.

(d) Folgern Sie aus (a) bis (c), dass für einen Primteiler p von $f(n)$, $n \in \mathbb{Z}$, entweder $p = 2$ oder $p \equiv 1, 4 \pmod{15}$ gilt.

(e) Zeigen Sie, dass ein Polynom $g(x) \in \mathbb{Z}[x]$ exisitiert, so dass $f(15x+1) = 15xg(x)+4$. Folgern Sie, dass alle Primteiler p von $f(15n+1)$ entweder gleich 2 oder kongruent zu 1 oder 4 modulo 15 sind und es mindestens einen Primteiler gibt, der $\equiv 4 \pmod{1)5}$ erfüllt, sofern n ungerade ist.

(f) Folgern Sie aus (e) die Behauptung

Lösung. (a) Da p nach Voraussetzung ungerade ist, folgt aus der Identität im Hinweis, dass für alle $n \in \mathbb{Z}$

$$(n^2 - n \cdot 2' - 1)^2 \equiv -15n^2 \cdot (2')^2 \pmod{p},$$

wobei $2' \in \mathbb{Z}$ mit $2 \cdot 2' \equiv 1 \pmod{p}$ sei. Diese Kongruenz kann nur dann gelten, wenn -15 ein Quadrat modulo p ist, also folgt nach dem quadratischen Reziprozitätsgesetz

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right),$$

wenn man noch beachtet, dass im Falle $p \equiv 3 \pmod{4}$ auch $\left(\frac{-1}{p}\right) = -1$ gilt. Damit ist entweder p gleichzeitig quadratischer Rest modulo 3 und 5 oder gleichzeitig quadratischer nichtrest zu beiden Moduln. Im ersten Fall folgt $p \equiv 1 \pmod{3}$ und $p \equiv \pm 1 \pmod{5}$, also nach dem Chinesischen Restsatz $p \equiv 1, 4 \pmod{15}$, im zweiten Fall gilt $p \equiv 2 \pmod{3}$ und $p \equiv \pm 2 \pmod{5}$, also folgt $p \equiv 2, 8 \pmod{15}$, woe behauptet.

(b) Analog zu (a).

(c) Analog zu (a).

(d) Aus (a), (b), (c) folgt, dass ein Primteiler p von $f(n)$ entweder 30 teilt (diese Primteiler hatten wir zu Beginn ausgeschlossen), oder $p \equiv 1, 4 \pmod{15}$ erfüllt. Es gilt für alle $n \in \mathbb{Z}$ nach dem kleinen Satz von Fermat

$$f(n) \equiv n^2 - n - n^2 + n + 1 \equiv 1 \pmod{3},$$

also $3 \nmid f(n)$ für alle n und durch Einsetzen der Restklassen findent man auch, dass $5 \nmid f(n)$ für alle n. Es bleibt also von den Ausnahmen nur $p = 2$ über. Wir bemerken an dieser Stelle, dass $2 \mid f(n)$ genau für ungerade n gilt.

(e) Es gilt $f(15n + 1) \equiv f(1) \equiv 4 \pmod{1}5$ für alle $n \in \mathbb{Z}$, also gibt es ein Polynom $\tilde{g} \in \mathbb{Z}[x]$ mit $f(15x + 1) = 15\tilde{g}(x) + 4$. Dieselbe Betrachtung modulo n liefert, dass $\tilde{g}(x) = xg(x)$ gelten muss, wie behauptet. In der Tat gilt

$$f(15x + 1) = 15x(3375x^3 + 675x^2 + 75x + 6) + 4.$$

Damit ist $f(15n + 1)$ für ungerades n ebenfalls ungerade, so dass nach (d) jeder seiner Primteiler 1 oder 4 modulo 15 ist, und es gilt $f(15x + 1) \equiv 4 \pmod{15}$, so dass mindestens einer dieser Primteiler $\equiv 4 \pmod{15}$ sein muss.

(f) Nehmen wir an, es gäbe nur endlich viele Primzahlen $p_1, ..., p_r$ der Form $15k + 4$ und sei N ihr Produkt. Dann ist insbesondere N ungerade. Damit besitst $f(15N +$

1) einen Primfaktor $q \equiv 4 \pmod{15}$. Nach (e) ist aber $f(15N+1) \equiv 4 \not\equiv 0 \pmod{p)_i}$ für $i = 1, ..., r$, so dass q mit keinem der p_i übereinstimmen kann, was den gewünschten Widerspruch liefert.

□