Übungen zur Elementaren Zahlentheorie

-3. Blatt (Alternative)-

Prof. Dr. K. Wingberg
J. Bartels

SS 2007
abzugeben bis Montag, den 14. Mai 2007

http://www.mathi.uni-heidelberg.de/~bartels/Uebungen.htm

Problem

In der Vorlesung wurden einige Spezialfälle des Dirichletschen Primzahlsatzes aufgeführt:
- Es gibt unendlich viele Primzahlen kongruent 2 mod 3.
- Es gibt unendlich viele Primzahlen kongruent 3 mod 4.

Dabei benutzten wir ein Argument ähnlich dem, welches in Euklids Satz vorkommt.
Entlang einer Arbeit aus den 60-er Jahren wollen wir hier allgemeiner das folgende Ergebnis etablieren:
In jeder der zu 24 primen Restklassen gibt es unendlich viele Primzahlen.

1 . Teil (Quadratisches Reziprozitätsgesetz)**:**
a) Zeige für prime $p > 3$ die folgenden Gleichungen:

$$I)\ \left(\frac{-2}{p}\right) = 1 \text{ genau dann, wenn } p \equiv 1, 3 (mod\ 8)$$

$$II)\ \left(\frac{3}{p}\right) = 1 \text{ genau dann, wenn } p \equiv 1, 11 (mod\ 12)$$

$$III)\ \left(\frac{-3}{p}\right) = 1 \text{ genau dann, wenn } p \equiv 1 (mod\ 6)$$

$$IV)\ \left(\frac{6}{p}\right) = 1 \text{ genau dann, wenn } p \equiv 1, 5, 19, 23 (mod\ 24)$$

$$V)\ \left(\frac{-6}{p}\right) = 1 \text{ genau dann, wenn } p \equiv 1, 5, 7, 11 (mod\ 24)$$

b) Es sei $n \in \mathbb{N}_{\geq 1}$ gegeben, dann ist jeder prime Teiler p von $n^8 - n^4 + 1$ kein Teiler der Zahlen $n^2, n^3 + n$ und $n^3 - n$.
Daraus folgere man die Existenz von Zahlen $a, b, c \in \mathbb{Z}$ mit

$$an^2 \equiv 1 (mod\ p)$$

$$b(n^3 + n) \equiv 1 (mod\ p)$$

$$c(n^3 - n) \equiv 1 (mod\ p)$$

2 . Teil (Fortsetzung)**:**
Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 - 1)^2 + (x^2)^2$ folgere man

$$(an^4 - a)^2 + 1 \equiv 0(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 + x^2 + 1)^2 - 2(x^3 + x)^2$ folgere man

$$(bn^4 + bn^2 + b)^2 - 2 \equiv 0(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 - x^2 + 1)^2 + 2(x^3 - x)^2$ folgere man

$$(cn^4 - cn^2 + c)^2 + 2 \equiv 0(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 + 1)^2 - 3(x^2)^2$ folgere man

$$(an^4 + a)^2 \equiv 3(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 - \frac{1}{2})^2 + 3(\frac{1}{2})^2$ folgere man

$$(2n^4 - 1)^2 \equiv -3(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 + 3x^2 + 1)^2 - 6(x^3 + x)^2$ folgere man

$$(bn^4 + 3bn^2 + b)^2 \equiv 6(mod\ p)$$

Aus der Zerlegung $x^8 - x^4 + 1 = (x^4 - 3x^2 + 1)^2 + 6(x^3 - x)^2$ folgere man

$$(cn^4 - 3cn^2 + c)^2 \equiv -6(mod\ p)$$

Aus obigem folgere man für einen Primteiler p von $n^8 - n^4 + 1$

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-6}{p}\right) = 1$$

und $p \equiv 1(mod\ 24)$.

Wir führen jetzt die folgenden Polynome ein:

$$f_5(x) = x^4 + 9 = (x^2)^2 + 3^2 = (x^2 + 3)^2 - 6x^2 = (x^2 - 3)^2 + 6x^2$$

$$f_7(x) = x^4 + 2x^2 + 4 = (x^2 + 2)^2 - 2x^2 = (x^2 + 1)^2 + 3 = (x^2 - 2)^2 + 6x^2$$

$$f_{11}(x) = x^4 + 4x^2 + 1 = (x^2 + 1)^2 + 2x^2 = (x^2 + 2)^2 - 3 = (x^2 - 1)^2 + 6x^2$$

$$f_{13}(x) = x^4 - x^2 + 1 = (x^2 - 1)^2 + x^2 = (x^2 - \frac{1}{2})^2 + 3(\frac{1}{2})^2 = (x^2 + 1)^2 - 3x^2$$

$$f_{17}(x) = x^4 + 1 = (x^2)^2 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 - 1)^2 + 2x^2$$

$$f_{19}(x) = x^4 - 2x^2 + 4 = (x^2 - 2)^2 + 2x^2 = (x^2 - 1)^2 + 3 = (x^2 + 2)^2 - 6x^2$$

$$f_{23}(x) = x^4 - 4x^2 + 1 = (x^2-1)^2 - 2x^2 = (x^2-2)^2 - 3 = (x^2+1)^2 - 6x^2$$

und weiter:

$$g_5(x) = \frac{1}{2} f_5(12x+1)$$
$$g_7(x) = f_7(6x+1)$$
$$g_{11}(x) = \frac{1}{3} f_{11}(6x+2)$$
$$g_{13}(x) = f_{13}(12x+2)$$
$$g_{17}(x) = f_{17}(6x+2)$$
$$g_{19}(x) = \frac{1}{12} f_{19}(12x+4)$$
$$g_{23}(x) = \frac{1}{2} f_{23}(12x+3)$$

3 . Teil :
Zeige, daß für $n \in \mathbb{N}$ und $l \in \{5, 7, 11, 13, 17, 19, 23\}$ folgendes gilt:
I) Jeder Primfaktor von $f_l(n)$ ist kongruent 1 oder l modulo 24.
II) Jeder Primfaktor von $g_l(n)$ ist kongruent l mod 24.

Jetzt der Schluß:

4 . Teil :
Ist l eine zu 24 teilerfremde Zahl, dann gibt es unendlich viele Primzahlen p, so daß

$$p \equiv l (mod\ 24)$$

gilt.