Übungen zur Elementaren Zahlentheorie

-2. Lösungsblatt-

Prof. Dr. K. Wingberg
J. Bartels

SS 2007

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

Lösung zum dritten Zettel

1 . Aufgabe :
Jede arithmetische Progression, die eine Quadratzahl und eine Kubikzahl enthält, enthält auch eine sechste Potenz.

Wir haben meinetwegen eine Progression

$$\{b + ak | k \in \mathbb{N}\},$$

die sowohl eine Quadratzahl als auch eine Kubikzahl enthält, d.h. es gibt $x, y \in \mathbb{Z}$ mit $x^2 \equiv y^3 \equiv b(mod\ a)$, für sie gilt $x^6 \equiv y^6 \equiv b^3(mod\ a)$. Sind a und y teilerfremd - dies ist gleichbedeutend mit der Teilerfremdheit von a und b, dann gibt es nach dem erweiterten Euklidischen Algorithmus $u \in \mathbb{Z}$, so daß $uy \equiv 1(mod\ a)$ gilt. (O.B.d.A. sei dies u positiv.) Dann ist $(uyx)^6 \equiv b^3(mod\ a)$ und $(ux)^6 \equiv b(mod\ a)$, was den Beweis im Fall der Teilerfremdheit von a und y zeigt.
Der schwierige Fall ist der, in der diese Teilerfremdheit nicht vorliegt: Man bedient sich einer Induktion nach a.
Für $a \leq n$ sei für jede Progression, die eine Quadrat- und eine Kubikzahl enthält, die Existenz einer sechsten Potenz in ihr bereits nachgewiesen.
Der Induktionsanfang für $n = 1, 2$ ist sofort klar.
Für $a = n + 1$ geht man folgendermaßen vor: Ist a teilerfremd zu b, dann ist alles bereits oben gezeigt. Es sei fortan daher $d := ggT(a, b) > 1$.
Für einen Primteiler p von d gilt, daß dieser entweder $\frac{a}{d}$ oder $\frac{b}{d}$ nicht teilt, gemäß der Definition des ggT.
Wenn $\frac{a}{d}$ nicht durch p geteilt wird, setzt man zunächst $i \in \mathbb{N}$ derart, daß $p^i || d$ gilt. Man hat dann die Kongruenzen

$$x^2 \equiv b(mod\ a/p^i) \text{ und } y^3 \equiv b(mod\ a/p^i).$$

Nach Induktuionsvoraussetzung gibt es dann ein $z \in \mathbb{N}$ mit $z^6 \in \{b + \frac{a}{p^i}k | k \in \mathbb{N}\}$. Der chinesische Restsatz zeigt das Vorkommen einer Zahl t mit

$$t \equiv z(mod\ \frac{a}{p^i})$$

und

$$t \equiv 0(mod\ p^i).$$

Für diese Zahl t gilt: t^6 ist in der Progression $\{b + ak | k \in \mathbb{N}\}$.
Es bleibt der Fall, daß p den Ausdruck $\frac{a}{d}$ teilt, also p^{i+1} in der Primfaktorzerlegung von a auftritt, also ist jedes Element der Progression durch p^i zu teilen, keines davon jedoch durch p^{i+1}. Insbesondere ist p^i die höchste $p-$Potenz, die in x^2 auftritt, gleiches gilt für y^3. die impliziert, daß i in $6\mathbb{Z}$ enthalten ist: $i = 6j$. Dann ist p^{3j} ein Teiler von x und p^{2j} einer von y. Desweiteren gilt $\frac{a}{p^{6j}} | (\left(\frac{x}{p^{3j}}\right)^2 - \left(\frac{b}{p^{6j}}\right))$, genauso $\frac{a}{p^{6j}} | (\left(\frac{y}{p^{2j}}\right)^3 - \left(\frac{b}{p^{6j}}\right))$. Wieder wendet man die Induktionshypothese an und findet ein $z \in \mathbb{N}$, so daß

$$z^6 \equiv \frac{b}{p^{6j}} (mod\ \frac{a}{p^{6j}}).$$

Dann ist $(zp^j)^6 - b)$ durch a zu teilen, was den Beweis vollendet.