Übungen zur Elementaren Zahlentheorie

-3. Blatt-

Prof. Dr. K. Wingberg
J. Bartels

SS 2007
abzugeben bis Montag, den 14. Mai 2007

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

Auf der oben genannten Seite ist ein alternativer Zettel zu finden, mithilfe dessen man eine Menge Restklassen modulo 24 untersucht. Wer diesen bearbeitet, braucht die ersten beiden Aufgaben dieses Zettels nicht mehr zu bearbeiten.

Übungsleiter:

Aufgabe	1	2	3	4	$\sum$
Punkte					

---

1 . Aufgabe (6 Punkte):
Nehmen wir an, eine Primzahl p sei kongruent 1 modulo 4, nach Lagrange also schreibbar in der Form $p = a^2 + b^2$, mit $a, b \in \mathbb{Z}$. Dabei sei a o.B.d.A. ungerade.
(Warum ist das eine legitime Annahme?)
Zeige:

$$\left(\frac{a}{p}\right) = 1$$

$$\left(\frac{(a+b)}{p}\right) = (-1)^{((a+b)^2-1)/8}$$

$$(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} (mod\ p)$$

$$(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} (mod\ p)$$

2 . Aufgabe (6 Punkte) (Fortsetzung)**:**
a) Ist f eine Zahl, so daß $b \equiv af(mod\ p)$, dann zeige man

$$f^2 \equiv -1(mod\ p)$$

und

$$2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}} (mod\ p)$$

b) Zeige, daß

$$x^4 \equiv 2(mod\ p)$$

für $p \equiv 1(mod\ 4)$ genau dann eine Lösung hat, wenn p die Form $C^2 + 64D^2$ hat, wobei C, D ganze Zahlen sind.

3 . Aufgabe (6 Punkte):
Es sei d eine positive natürliche Zahl mit $d \notin \{2, 5, 13\}$. Zeige, daß es in der Menge $\{2, 5, 13, d\}$ zwei Zahlen a, b gibt, so daß $ab - 1$ keine Quadratzahl ist.

Wir haben in der Vorlesung Restklassen modulo b - also arithmetische Progressionen, d.h. zu gegebenem a, b Mengen der Form $\{a + b.n | n \in \mathbb{N}\}$, untersucht.

4 . Aufgabe (6 Punkte):
Jede arithmetische Progression, die eine Quadratzahl und eine Kubikzahl enthält, enthält auch eine sechste Potenz.