Notre Dame Journal of Formal Logic
Volume XVII, Number 1, January 1976
NDJFAM

ÜBER KONGRUENZEN HÖHERER OPERATIONEN

GÜNTHER FREI-IMFELD

1* Im Anschluss an die Arbeit [1] stellt sich die natürliche Frage, wann die Kongruenz $x^x \equiv a$ modulo m mit m und a als ganze, teilerfremde Zahlen lösbar ist. Diese Frage läßt sich mit Hilfe einfacher elementarzahlentheoretischer Hilfsmittel beantworten. Das Hauptresultat bildet der Satz 4.

2 Beginnen wir mit einem Resultat, das sich unmittelbar aus der Tatsache ergibt, daß in $b^e \equiv a \pmod{m}$ die Basis b modulo m und der Exponent e modulo $\psi(m)$ [oder modulo einem Teiler von $\psi(m)$] bestimmt ist, wobei $\psi(m)$ die verallgemeinerte Eulersche Funktion darstellt, d.h. $\psi(m)$ ist der kleinste Exponent e, derart daß $b^e \equiv 1 \pmod{m}$ für alle zu m teilerfremden b gilt. $\psi(m)$ ist gleich der Eulerschen Funktion $\varphi(m)$, falls m Primitivwurzeln zuläßt, d.h. falls m gleich einer der Zahlen 1, 2, 4, p^α, $2p^\alpha$ ist, wo p eine ungerade Primzahl und α eine natürliche Zahl bedeutet; sonst ist $\psi(m)$ ein echter Teiler von $\varphi(m)$. Es seien nun durchwegs m, a und r beliebige ganze Zahlen, wobei stets a und r als zu m teilerfremd angenommen seien. Die Ordnung von r modulo m sei h. Natürlich ist h ein Teiler von $\psi(m)$. Ferner sei $s = \dfrac{h}{(m, h)}$ und $\sigma = \dfrac{m}{(m, h)}$, wo (m, h) der g.g.T. von m und h bedeute. Ist $[m, h]$ das k.g.V. von m und h, so hat man also $[m, h] = \dfrac{mh}{(m, h)} = ms = \sigma h$.

Nun haben wir den

Satz 1 (i) *Die simultanen Kongruenzen*

$$x^x \equiv a \pmod{m}$$
$$x \equiv r \pmod{m}$$

sind genau dann lösbar, wenn

$$a \equiv r^{r+mu} \pmod{m} \text{ ist, mit } 0 \leq u < s;$$

*Die Arbeit wurde gefördert durch NRC Grant Nr. A 7842.

Received September 3, 1974