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 $s = \frac{h}{(m, h)}$ und $\sigma = \frac{m}{(m, h)}$, 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 $[m, h] = \frac{mh}{(m, h)} = ms = \sigma h$.

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

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

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

Received September 3, 1974

(ii) *Die Lösung ist dann eindeutig modulo* $[m, h] = ms$.

Beweis: (i) Ist $a \equiv r^{r+mu} \pmod{m}$ mit $0 \leq u < s$, dann folgt $a \equiv (r + mu)^{(r+mu)} \pmod{m}$, also sind die Kongruenzen lösbar. Ist umgekehrt $x^x \equiv a \pmod{m}$ und $x \equiv r \pmod{m}$ lösbar für ein $x = t$, dann ist $t = r + my$ für ein $y \in Z$, wobei y in die Form $y = u + sz$, mit $z \in Z$ und $0 \leq u < s$, gesetzt werden kann. Somit ist

$$a \equiv t^t \equiv (r + my)^{(r+my)} \equiv r^{r+mu} r^{zms} \equiv r^{r+mu} r^{z\sigma h} \equiv r^{r+mu} \pmod{m}.$$

(ii) Sind t_1 und t_2 zwei Lösungen mit

$$t_1 = r + m\,(u_1 + z_1 s) \text{ für ein } u_1 \text{ mit } 0 \leq u_1 < s \text{ und ein } z_1 \in Z,$$

und

$$t_2 = r + m\,(u_2 + z_2 s) \text{ für ein } u_2 \text{ mit } 0 \leq u_2 < s \text{ und ein } z_2 \in Z,$$

dann folgt aus $a \equiv r^{r+mu_1} \equiv r^{r+mu_2} \pmod{m}$, daß $mu_1 \equiv mu_2 \pmod{h}$ und nach Division mit (m, h), daß $\sigma u_1 \equiv \sigma u_2 \pmod{s}$ sein muß. Wegen $(\sigma, s) = 1$ ergibt sich daraus $u_1 = u_2$, also ist $t_1 \equiv t_2 \pmod{ms}$.

Bemerkung: Die $r^{r+mu} \pmod{m}$ mit $0 \leq u < s$ sind alle inkongruent modulo m, wie aus dem Beweis hervorgeht.

3 Gemäß dem chinesischen Restsatz kann die Lösung der beiden simultanen Kongruenzen modulo m in Satz 1 auf ein System von Lösungen von paarweisen simultanen Kongruenzen modulo den Primpotenzteilern von m zurückgeführt werden. Für die Lösbarkeit dieser Kongruenzen werden wir in Satz 4 befriedigende Kriterien finden. Zunächst benötigen wir den folgenden

Hilfssatz 2 *Ist p eine Primzahl und r eine nicht durch p teilbare ganze Zahl der Ordnung h modulo p, dann gilt*

$$r^{p^\gamma h} \equiv 1 \pmod{p^{\gamma+1}} \text{ für jedes } \gamma = 0, 1, 2, \ldots .$$

Beweis: mit vollständiger Induktion nach γ.

N_0) $r^h \equiv 1 \pmod{p}$ gemäß Voraussetzung.
$N \to N + 1$) Gilt die Behauptung für alle β mit $0 \leq \beta \leq \gamma$, also speziell $r^{p^\gamma h} \equiv 1 \pmod{p^{\gamma+1}}$, dann ist $r^{p^\gamma h} = 1 + yp^{\gamma+1}$ für ein $y \in Z$.

Somit ist $r^{p^{\gamma+1} h} \equiv (1 + yp^{\gamma+1})^p \equiv 1 \pmod{p^{\gamma+2}}$.

Weiter benötigen wir den

Satz 3 *Es sei p eine beliebige Primzahl und r und t zwei nicht durch p teilbare ganze Zahlen. Ferner sei h die Ordnung von r modulo p. Dann folgt aus $t \equiv r \pmod{p}$ und $t \not\equiv r \pmod{p^\alpha h}$ daß $t^t \not\equiv r^r \pmod{p^\alpha}$ ist.*

Beweis: Den Beweis führen wir mit vollständiger Induktion nach α.

N_0) a) Im Falle $\alpha = 1$ seien t und r so beschaffen, daß $t \equiv r \pmod{p}$ aber $t \not\equiv r \pmod{ph}$ gelte, wobei zunächst $h \geq 2$ vorausgesetzt sei. Dann gibt es ein $z \in Z$ und ein f mit $1 \leqslant f < h$, so daß $t = r + p\ (f + zh)$ ist, und man hat

$$t^t \equiv r^{r+pf} \equiv r^r (r^p)^f \equiv r^r r^f \not\equiv r^r \pmod{p}$$

wegen des Satzes von Fermat und weil $f \neq 0$ sein muß, wegen $t \not\equiv r \pmod{ph}$. Ferner muß gemäß Voraussetzung $r \not\equiv 1 \pmod{p}$ sein, weil sonst $h = 1$ wäre.

b) Ist nun aber $h = 1$, dann wird die Voraussetzung falsch, also ist die Aussage des Satzes in diesem Falle ebenfalls richtig.

$N \to N + 1$) Die Behauptung gelte jetzt für alle α mit $1 \leqslant \alpha \leqslant \gamma$. Setzen wir $\alpha = \gamma + 1$ mit $\gamma \geqslant 1$, dann gilt die Voraussetzung $t \equiv r \pmod{p}$ und $t \not\equiv r \pmod{p^{\gamma+1}h}$. Wir unterscheiden zwei Fälle:

a) Ist $t \not\equiv r \pmod{p^\gamma h}$ dann ist nach Induktionsvoraussetzung $t^t \not\equiv r^r \pmod{p^\gamma}$ also auch $t^t \not\equiv r^r \pmod{p^{\gamma+1}}$.

b) Ist $t \equiv r \pmod{p^\gamma h}$, dann gibt es ganze Zahlen c und z, so daß $t = r + p^\gamma hc + p^{\gamma+1}hz$ und $c \not\equiv 0 \pmod{p}$ ist. Dann muß auch $hc \not\equiv 0 \pmod{p}$ sein. Wegen Hilfssatz 2 hat man jetzt

$$t^t \equiv (r + p^\gamma hc)^r \pmod{p^{\gamma+1}}.$$

Entwickelt man die rechte Seite, so hat man wegen $r \not\equiv 0 \pmod{p}$ und $\gamma \geqslant 1$:

$$t^t \equiv r^r + r^r p^\gamma hc \equiv r^r(1 + p^\gamma hc) \not\equiv r^r \pmod{p^{\gamma+1}},$$

weil $hc \not\equiv 0 \pmod{p}$ ist.

4 Jetzt können wir das folgende Hauptresultat herleiten.

Satz 4 *Es sei p eine beliebige Primzahl und a und r zwei nicht durch p teilbare ganze Zahlen. Ferner sei h die Ordnung von r modulo p.*

(i) *Dann sind die simultanen Kongruenzen*

$$x^x \equiv a \pmod{p^\alpha},\ (\alpha \geqslant 1)\ \textit{und}\ x \equiv r \pmod{p}$$

genau dann lösbar, wenn eine der zwei folgenden äquivalenten Bedingungen erfüllt ist:

(1) *a ist $\frac{p-1}{h}$ - ter Potenzrest modulo p^α.*

(2) $a^{p^{\alpha-1}h} \equiv 1 \pmod{p^\alpha}$.

(ii) *Die Lösung ist dann eindeutig modulo $p^\alpha h$.*

Beweis: (i) Daß die Bedingungen (1) und (2) gleichwertig sind, folgt aus dem verallgemeinerten Eulerschen Kriterium, wonach a genau dann $\frac{p-1}{h}$-ter Potenzrest modulo p^α ist, wenn $a^d \equiv 1 \pmod{p^\alpha}$ ist, wobei

$$d = \frac{\varphi(p^\alpha)}{\left(\frac{p-1}{h}, \varphi(p^\alpha)\right)} = p^{\alpha-1}\ h$$

ist. Die Notwendigkeit der Bedingungen folgt jetzt sofort, denn ist $x = t$ eine Lösung der beiden Kongruenzen, dann ist nach Hilfssatz 2

$$a^{p^{\alpha-1}h} \equiv (t^t)^{p^{\alpha-1}h} \equiv (t^{p^{\alpha-1}h})^t \equiv 1 \pmod{p^\alpha}.$$

Daß die Bedingungen auch hinreichend sind folgt so: Es sei $t_u = r + up$ mit $0 \leqslant u \leqslant p^{\alpha-1}h$. Dann sind nach Satz 3 die $t_u^{t_u}$ für die $p^{\alpha-1}h$ verschiedenen Werte von u alle inkongruent modulo p^α. Nach dem Vorangehenden sind die $t_u^{t_u}$ allesamt $\frac{p-1}{h}$-te Potenzreste modulo p^α. Nun gibt es aber genau $\frac{\varphi(p^\alpha)}{\frac{p-1}{h}} = p^{\alpha-1}h$ solche $\frac{p-1}{h}$-te, inkongruente Potenzreste modulo p^α, denn p^α besitzt eine Primitivzahl. Damit stellen die $t_u^{t_u}$ mit $0 \leqslant u \leqslant p^{\alpha-1}h$ alle $\frac{p-1}{h}$-ten Potenzreste modulo p^α je genau einmal dar.

Also sind die Bedingungen hinreichend, und gleichzeitig ist auch (ii) bewiesen.

Wir wollen noch den Spezialfall, wo $r = g$ eine Primitivzahl modulo p ist, besonders vermerken:

Satz 5 *Ist a eine beliebige ganze Zahl, die nicht durch die Primzahl p teilbar ist, und ist g eine Primitivzahl modulo p, dann sind die simultanen Kongruenzen*

$$x^x \equiv a \pmod{p^\alpha},\ (\alpha \geqslant 1) \textit{ und } x \equiv g \pmod{p}$$

stets eindeutig modulo $p^\alpha(p-1)$ lösbar.

LITERATURVERZEICHNIS

[1] Frei-Imfeld, G., "Über eine Erweiterung der algebraischen Operationen," *Notre Dame Journal of Formal Logic*, vol. XV (1974), pp. 279-288.

Université Laval
Québec, Québec, Canada