Diskrete Mathematik
Kongruenzen

Ellen Hentschel
Thomas Gaub

31. Mai 2006

Inhaltsverzeichnis

Einleitung

Fragestellung

Wie rechnet man mit Zahlen, die bei der Division durch eine dritte Zahl den selben Rest haben?

Kongruenz

Definition:
Zwei Zahlen a und b heissen kongruent modulo m (m≠0), wenn b-a ein Vielfaches von m ist, also m|b-a.
Schreibweise:a≡b mod m

Bemerkung

1. Zu einander kongruente Zahlen lassen bei der Division durch m den gleichen Rest

2. Zwei Zahlen die nicht den gleichen Rest lassen heissen inkongruent modulo m.

Beispiele

$$25 \equiv -3 \bmod 4$$

$$(-3)-25 = -28 \quad 4 \mid -28$$

$$25 = 1 \bmod 4$$

$$-3 = 1 \bmod 4$$

$$7 \equiv 42 \bmod 5$$

$$42-7 = 355 \mid 35$$

$$42 = 2 \bmod 5$$

$$7 = 2 \bmod 5$$

Bemerkung

1. $a \equiv 0 \bmod m \Leftrightarrow m \mid a$
2. $a = b \Leftrightarrow a \equiv b \bmod m$ für alle m
3. $a \equiv b \bmod 1$ für alle a und b
4. $a \equiv b \bmod mn \Rightarrow a \equiv b \bmod m$

Kongruenz ist eine Äquivalenzrelation.

1. reflexiv

$$a \equiv a \bmod m$$

2. symetrisch

$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$$

3. transitiv

$$a \equiv b \bmod m,\ b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$$

Restklassen

Die ganzen Zahlen zerfallen mit der Kongruenz also in Äquivalenzklassen, die Restklassen modulo m.

Jede Zahl fällt genau in eine Klasse.
=> Angabe einer Zahl reicht um Restklasse eindeutig zu bestimmen.

$$[a]_m = \{x \mid x \equiv a \bmod m\}$$

Vollständiges Restsystem

Eine Menge von Zahlen, die aus jeder Restklasse genau eine Zahl enthält, heisst „vollständiges Restsystem“

Satz:
$\{r_1, r_2, \ldots, r_m,\}$ vollständig Restsystem <=>
Aus $r_i \equiv r_k$ folgt stets $i=k$.

Beispiel

{0,1,2,3,4} ist vollständiges Restsystem modulo 5
genau wie {a,a+1, a+2,a+3,a+4}

$\{r_1, r_2, \ldots, r_m\}$ vollständiges Restsystem =>
$\{a+r_1, a+r_2, \ldots, a+r_m\}$ vollständiges Restsystem

gilt (a,m)=1 :
$\{r_1, r_2, \ldots, r_m\}$ vollständiges Restsystem =>
$\{ar_1, ar_2, \ldots, ar_m\}$ vollständiges Restsystem

Sind $\{r_1, \ldots, r_m\}$ und $\{s_1, s_2, \ldots s_n\}$ vollständige Restsysteme modulo m bzw. n, und (m,n)=1, dann ist $\{nr_i+ms_j, \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ ein vollständiges Restsystem mn

Beweis

Sei

$$ms_{i_1} + nr_{j_1} \equiv ms_{i_2} + nr_{j_2} \bmod mn$$

$$\Rightarrow \quad nr_{j_1} \equiv nr_{j_2} \bmod m$$

$$\Rightarrow \quad r_{j_1} \equiv r_{j_2} \bmod m$$

$$\Rightarrow \quad j_1 \equiv j_2$$

Inverse modulo m

Seien a und n teilerfremde Zahlen dann gibt es eine Zahl a' ϵ {1,2,3, ... n-1} mit a * a' ≡ 1 mod n.

Die Zahl a' heißt Inverse von a modulo n

Beweis

Es ist

$$1 = a * a' + n * b'$$

also

$$1 \equiv a * a' \bmod m$$

Ist a'>n oder a' ≤ 0 so ist a' = a'' +k*n mit a'' ϵ {1,2, .. n-1} und damit

1 = a*(a'' + k*n) + n*b ≡ a * a'' mod n

Rechenregeln

Vor.: $a \equiv b \bmod m$ und $c \equiv d \bmod m$

$$a+c \equiv b+d \bmod m$$
$$ac \equiv bd \bmod m$$

$$a^n \equiv b^n \bmod m$$

Anwendung

Ist $2^{32}+1$ eine Primzahl

Bekannt $641 = 5*2^7+1$

Also $5*2^7 \equiv -1 \bmod 641$

$(5*2^7)^4 \equiv (-1)^4 \bmod 641$

$5^4 * 2^{28} \equiv 1 \bmod 641$

weiter hin gilt $5^4 + 2^4 = 641$ und damit $5^4 \equiv -2^4 \bmod 641$

Also $-2^4 * 2^{28} \equiv 1 \bmod 641$

$-2^{32} \equiv 1 \bmod 641$

$2^{32} \equiv -1 \bmod 641$

und damit $641 \mid 2^{32}+1$

Übung 1

Zeige
$8L + 7 \neq x^2 + y^2 + z^2$
oder $x^2 + y^2 + z^2$ inkongruent 7 modulo 8
Tip: Betrachte die Kongruenzen von x^2

Lösung

Reste r von x^2 mod 8:
0,1,4
Gleiche Reste bei y^2 und z^2
Also hat $x^2 + y^2 + z^2$ die möglichen Reste
0,1,2,3,4,5,6. Und damit nicht 7
q.e.d

Polynome

Satz:
Für jedes Polynom P(x) gilt: Ist a≡b mod m, so auch P(a)≡P(b) mod m

Definition:
Die Lösungszahl von P(x)≡k mod m ist die Anzahl der Restklassen modulo m , in die Lösungsmenge zerfällt

Division ?

16≡2 mod 14 | :2
8≡1 mod 14 offensichtlich falsch!

Also Division im Allgemeinen nicht erlaubt

Division

Division ist allerdings erlaubt wenn der Divisor c ein Faktor des Moduls ist
ac≡bc mod m|c| => a≡b mod m

Ist der Divisor kein Faktor des Moduls gilt:

$$ac \equiv bc \bmod m \Rightarrow \quad a \equiv b \bmod \frac{m}{(m,c)}$$

Übung 2

Berechnen Sie 30≡ 2 mod 7 :2
und 21 ≡ 35 mod 14 : 7

Prime Restklassen

Prime Restklassen

Eine Restklasse $[a]_m$ heißt zu m prime Restklasse, wenn $([a]_m, m) = 1$.

Das heißt, dass ein beliebiger Repräsentant – und somit alle Repräsentanten – teilerfremd zum Modul ist.

Beispiel:

$([7]_{10}, 10) = 1$

zur Erinnerung:

$[a]_m = \{x \mid x \equiv a \bmod m\}$

der ggT eine Restklasse

$$a \equiv b \bmod m \Rightarrow (a,m) = (b,m)$$

- Beispiel: a = 16 , b = 6, m = 10

  $\Rightarrow 16 \equiv 6 \bmod 10$

  $\Rightarrow (16,10) = 2$

  $\Rightarrow (6,10) = 2$

- Beweis:

  $a = qm + b$

  $a = q * m' * (b,m) + b' * (b,m)$

  $\Rightarrow$ (b,m) teilt auch a

  $\Rightarrow$ es gibt keinen größeren Teiler für a

  $\Rightarrow (a,m) = (b,m)$

- Somit ist mit einem Repräsentanten der ggT für alle Zahlen dieser Restklasse definiert.

Eulersche φ - Funktion

Sei $\varphi(m) = \#\{a \mid 1 \leq a \leq m \text{ und } (a,m) = 1\}$

$\varphi(m)$ gibt also die Anzahl der teilerfremden Zahlen und somit die Anzahl der primen Restklassen an.

$\{a \mid 1 \leq a \leq m \text{ und } (a,m) = 1\}$ wird primes Restsystem genannt.

Sind $\{r_1, r_2, ..., r_{\varphi(m)}\}$ und $\{s_1, s_2, ..., s_{\varphi(m)}\}$ prime Restsysteme modulo m bzw. n mit (m, n) = 1, dann ist $\{ms_i + nr_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ primes Restsystem modulo m * n.

Für die Anzahl der teilerfremden Elemente von m*n ergibt sich:

$$\varphi(mn) = \varphi(m) * \varphi(n) \quad \text{für } (m,n) = 1$$

Beispiel

$m = 6 \Rightarrow \{r_1, r_2\} = \{1,5\}, \ \varphi(6) = 2$

$n = 5 \Rightarrow \{s_1, s_2, s_3, s_4\} = \{1,2,3,4\}, \ \varphi(10) = 4$

$nm = 30 \Rightarrow \{6s_i + 5r_j \mid 1 \leq i \leq \varphi(5), 1 \leq j \leq \varphi(6)\} \bmod 30$

$6 + 5$	$= 11$	$\bmod 30$	$= 11$
$6 + 25$	$= 31$		$= 1$
$12 + 5$	$= 17$		$= 17$
$12 + 25$	$= 37$		$= 7$
$18 + 5$	$= 23$		$= 23$
$18 + 25$	$= 43$		$= 13$
$24 + 5$	$= 29$		$= 29$
$24 + 25$	$= 49$		$= 19$

$\{1,7,11,13,17,19,23,29\}, \ \varphi(30) = \varphi(6) * \varphi(5) = 8$

Übung 3

Bilden Sie aus den primen Restsystemen modulo 3 und 4 das prime Restsystem modulo 12 und geben Sie jeweils die φ - Funktion an.

Übung 3

Bilden Sie aus den primen Restsystemen modulo 3 und 4 das prime Restsystem modulo 12 und geben Sie jeweils die φ - Funktion an.

Lösung:

M = 3 => {1,2} $\varphi(3) = 2$
N = 4 => {1,3} $\varphi(4) = 2$
=> M * N = 3 * 4 = 12= {1,5,7,11} $\varphi(3) * \varphi(4) = \varphi(12) = 4$

φ - Funktion von Primzahlen

Sei p eine Primzahl, so ist

$$\varphi(p) = p - 1$$ (nämlich die Zahlen von 1 bis p – 1)

und

$$\varphi(p^e) = p^e * (1 - 1/p)$$

Beweis

Die teilerfremden Zahlen zu p^e sind alle Zahlen außer den Vielfachen von p.

Die Vielfachen von p:

$$M = \{p, 2p, ..., p^{e-1} * p\}$$

Anzahl der Vielfachen von p:

$$|M| = p^{e-1}$$

Also ist

$$\varphi(p^e) = p^e - p^{e-1}$$
$$= p^e * (1 - 1/p)$$

Berechnung der φ - Funktion einer beliebigen Zahl

Die φ - Funktion lässt sich aufgrund der Primfaktorzerlegung berechnen durch:

$$\varphi(n) = n * \prod_{i=1}^{r} (1 - 1/p_i) = n * \prod_{p|n} (1 - 1/p_i)$$

Übung 4

Beweisen Sie $\varphi(n) = n * \prod^{r}_{i=1} (1 - 1/p_i) = n * \prod_{p|n} (1 - 1/p_i)$!

Übung 4

Beweisen Sie $\varphi(n) = n * \prod_{i=1}^{r} (1 - 1/p_i) = n * \prod_{p|n} (1 - 1/p_i)$!

Lösung:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{e1} * p_2^{e2} * \ldots * p_r^{er}) \\
&= \varphi(p_1^{e1}) * \ldots * \varphi(p_r^{er}) \\
&= p_1^{e1} * (1 - 1/p_1) * p_2^{e2} * (1 - 1/p_2) * \ldots * p_r^{er} * (1 - 1/p_r) \\
&= n * \prod_{i=1}^{r} (1 - 1/p_i) \\
&= n * \prod_{p|n} (1 - 1/p_i)
\end{aligned}$$

Die Summe der eulerschen φ - Funktionen aller positiven Teiler einer Zahl n ergibt wiederum diese Zahl, also

$$\sum_{d|n,d>0} \varphi(d) = n$$

Beispiel:
n = 6

$$\{1,2,3,6\} = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$$

Die Sätze von Euler und Fermat

Satz von Euler

Ist (a,m) = 1, dann gilt
$$a^{\varphi(m)} \equiv 1 \bmod m$$

Die Menge {a|1≤a≤m und (a,m) = 1 } bildet eine multiplikative Gruppe mit Gruppenordnung φ(m), gilt für jedes Element der Gruppe, das es hoch φ(m) das neutrale Element ergibt.

Kleiner Satz von Fermat

Ist p Primzahl und a positiv, so ist
$$a^{p-1} \equiv 1 \bmod p \text{ bzw.}$$
$$a^{p} \equiv a \bmod p$$

Lineare Kongruenzen

lineare Kongruenzen

$$a * x \equiv k \bmod m$$

Die Lösung dieser Gleichung ist entweder

Ø , falls (a,m) k nicht teilt

oder

eine Restklasse mod (m/(a,m)) sonst

Beweis

$$a * x \equiv k \bmod m$$
$$a * x - k = m * y$$
$$a * x - m * y = k$$

Ist der ggT (a,m) kein Teiler der rechten Seite, so ist das System unlösbar, ansonsten eine Restklasse mod $\frac{m}{(a\,,\,m)}$.

<u>betrachte hierzu diophantische Gleichungen:</u>

ax + by = k hat eine ganzzahlige Lösung, falls (a,b)| k.

Übung 5

Sind folgende Gleichungen lösbar? Wenn ja, wie könnte man die Gleichung nach x auflösen?

$3 * x \equiv 2 \bmod 9$

$16 * x \equiv 14 \bmod 6$

Übung 5

Sind folgende Gleichungen lösbar? Wenn ja, wie könnte man die Gleichung nach x auflösen?

$3 * x \equiv 2 \bmod 9$

$16 * x \equiv 14 \bmod 6$

Lösung:

1) (3,9) = 3 teilt nicht 2 => nicht lösbar
2) (16,6) = 2 | 14 => lösbar

$8 * x \equiv 7 \bmod 3$

$-x \equiv 7 \bmod 3$

$x \equiv -7 \bmod 3$

$x \equiv 2 \bmod 3$

Strukturierte Lösung der Gleichung

Zunächst dividieren wir die Gleichung durch (a,m).

$$\frac{a}{(a,m)} \cdot x \equiv \frac{k}{(a,m)} \bmod \frac{m}{(a,m)}$$

oder neu benannt $a_1 * x \equiv k_1 \bmod m_1$

Somit ist $(a_1 , m_1) = 1$ und damit $a_1^{\varphi(m1)} \equiv 1 \bmod m_1$

Mit $x = k_1 * a_1^{\varphi(m1) - 1}$ existiert nun eine Lösung, denn

$$a_1 * x = k_1 * a_1^{\varphi(m1)} \equiv k_1 \bmod m_1$$

Beispiel

$$16 * x \equiv 14 \bmod 6$$

ist lösbar, da (16,6) | 14 . Teilt man nun durch den ggT (= 2) ergibt sich:

$$8 * x \equiv 7 \bmod 3$$

Damit ist

$$x = k_1 * a_1^{\varphi(m1) - 1} = 7 * 8^{2-1} = 56$$

eine Lösung.

$$x = 56 \equiv 2 \bmod 3$$

Wie findet man nun die gesamte Lösungsmenge?

Aus der ggT-Theorie wissen wir, dass die Gleichung

$$ax + qm = k$$

folgende Lösungen hat, wobei x eine bekannte Lösung bezeichnet:

$$x_t = x + \frac{m}{(a, m)} * t \text{ , } t = 0,1, \ldots$$

$$\begin{aligned} & ax + qm = k \\ \Leftrightarrow \quad & ax = -qm + k \\ \Leftrightarrow \quad & ax \equiv k \bmod m \end{aligned}$$

Somit sind die x_t auch Lösung von $ax \equiv k \bmod m$.

Beispiel

Wir wissen, dass $x = 56 \equiv 2 \bmod 3$

und $x \equiv 2 \bmod 3 \iff 16x \equiv 14 \bmod 6$

Wie muss k aussehen, damit es die Gleichung $x = 56 \equiv k \bmod 6$ erfüllt? $\Rightarrow k = 2$

Also existieren folgende Lösungen:

$x \equiv 2 \bmod 6$ $\quad x_0 = 2 + \frac{6}{(16,6)} * 0 = 2 + 3 * 0 = 2$

$x \equiv 5 \bmod 6$ $\quad x_1 = 2 + 3 * 1 = 5$

$x_2 = 2 + 3 * 2 = 8 \bmod 6 = 2 = x_0$

Anzahl der Lösungen

Die Lösungsanzahl von $ax \equiv k \bmod m$ ist für $(a,m) \mid k$ gleich (a,m).

Beweis

$x_t = x + \frac{m}{(a,m)} * t$, $t = 0,1, \ldots$ lösen die Gleichung $ax \equiv k \bmod m$.

Also müssen zwei auf diese Weise gewonnene Lösungen gleich modulo m sein:

$$x + \frac{m}{(a,m)} * t_1 \equiv x + \frac{m}{(a,m)} * t_2 \bmod m$$

$$t_1 \equiv t_2 \bmod \left(m * \frac{(a,m)}{m}\right)$$

$$t_1 \equiv t_2 \bmod (a,m)$$

k mod (a,m) hat genau (a,m) Reste, nämlich 0, 1, ..., (a,m) – 1. Somit kann t (a,m) Werte annehmen, ohne dass sich die Ergebnisse wiederholen.

Zusammenfassung

1. Schritt: eine Lösung suchen

$$x = k_1 * a_1^{\varphi(m1) - 1} \quad \text{mit } m_1 = \frac{m}{(a, m)}, k_1 = \frac{k}{(a, m)}, a_1 = \frac{a}{(a, m)}$$

2. Schritt: alle Lösungen berechnen

$$x_t = x + \frac{m}{(a, m)} * t, t = 0,1, \ldots, (a,m) - 1$$

Systeme

Systeme

Betrachten wir das System

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

mit (m,n) =1 und alle Zahlen nicht negativ

.

Dann existiert eine eindeutige Lösung für x in {0,1,2, ... ,mn-1}

Bew: $x = a*n^{\varphi(m)} + b*m^{\varphi(n)}$ erfüllt beide Gleichungen (trivial)

Allgemeiner

Wie löst man
$x \equiv a \bmod m$
$x \equiv b \bmod n$
mit $(m,n) = d$?

$$x = k*m + a$$
$$y = l*n + b$$

$$\Rightarrow k*m - l*n = b-a$$

$$\Rightarrow (m,n) | (b-a) \text{ und damit } b-a = u*(m,n)$$

Also eine Lösung des Ursprünglichen Systems

$$k_1*m - l_1*n = (m,n)$$

$$k_1 * m - l_1 * n = (m,n)$$

$$u * k_1 * m - u * l_1 * n = (m,n) * u = b - a$$

$$\text{Und damit } k = u * k_1 \text{ und } l = u * l_1$$

$$\text{also } x = u * k_1 * m + a \text{ bzw. } x = u * l_1 * n + b$$

Übung 6

Berechnen Sie eine Lösung von
$$x \equiv 7 \bmod 20$$
$$x \equiv 11 \bmod 56$$

Lösung

(20,56)= 4 mit 4 = 3*20 -1* 56
Da 4|(11-7) ist das System lösbar und u = 1
Und damit
x = 3*20 + 7 = 67
bzw.
x = 1*56 + 11 = 67