Reste sind doch das Beste

– Geheimnisvolle Modulorechnung –

Martin Kreuzer

Universität Passau

martin.kreuzer@uni-passau.de

Lehrerfortbildung

"Top Secret - Geheimnisvolle Berechnungen"

Universität Passau, 15.12.2023

Inhaltsübersicht

1. **Grundlagen der Resterechnung**
2. **Der chinesische Restsatz**
3. **Der kleine Satz von Fermat**
4. **Der Satz von Euler**
5. **Fortgeschrittene Resterechnung**

Idee der LFB: Material und Tipps für den neuen Modul

Zahlentheorie und Kryptologie.

§1. Grundlagen der Resterechnung

Dass sie von dem Sauerkohle
Eine Portion sich hole,
Wofür sie besonders schwärmt,
Wenn er wieder aufgewärmt.
(Wilhelm Busch)

Satz (Teilen mit Rest)

Sei $n \in \mathbb{N}_+$. Dann besitzt jede ganze Zahl $z \in \mathbb{Z}$ eine Darstellung

$$z = q \cdot n + r \qquad \text{mit } q, r \in \mathbb{Z} \text{ und } 0 \leq r < n.$$

Hierbei heißt r der **Rest** *von z* **modulo** *n.*

Definition

Sei $n \in \mathbb{N}_+$ und seien $z_1, z_2 \in \mathbb{Z}$. Schreibe $z_1 = q_1\, n + r_1$ und $z_2 = q_2\, n + r_2$ mit $q_1, q_2 \in \mathbb{Z}$ und $r_1, r_2 \in \{0, 1, \ldots, n-1\}$.

(a) Die Zahlen z_1, z_2 heißen **kongruent modulo** n, wenn $r_1 = r_2$ gilt. In diesem Fall schreiben wir

$$z_1 \equiv z_2 \pmod{n}$$

(b) Die Menge $\bar{z}_1 = \{z_2 \in \mathbb{Z} \mid z_2 \equiv z_1 \pmod{n}\}$ heißt die **Restklasse** von z_1 modulo n.

Bemerkung

Die Restklassen modulo n sind: $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\}$

Ziel: Rechne mit Restklassen!

Definition (Addition von Restklassen)

Sei $n \in \mathbb{N}_+$ und seien $z_1, z_2 \in \mathbb{Z}$. Dann setzen wir

$$\bar{z}_1 + \bar{z}_2 \;=\; \overline{z_1 + z_2}.$$

Das heißt, man addiert zwei Restklassen modulo n wie folgt:

(1) Wähle eine Zahl z_1 aus der ersten Restklasse.

(2) Wähle eine Zahl z_2 aus der zweiten Restklasse.

(3) Berechne $s = z_1 + z_2$. Dann ist $\bar{s}$ die Summe der beiden Restklassen.

Beispiel

(a) In $\mathbb{Z}/5\mathbb{Z}$ gilt $\overline{-1} = \bar{9}$ und $\overline{-1} + \bar{9} = \bar{3}$.

(b) In $\mathbb{Z}/2\mathbb{Z}$ gibt es nur zwei Restklassen $\bar{0}$ und $\bar{1}$. Es gilt $\bar{0} + \bar{0} = \bar{1} + \bar{1} = \bar{0}$ sowie $\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$.

Satz

Die Addition von Restklassen ist **wohldefiniert**, *d.h. sie ist unabhängig von der speziellen Wahl der* **Repräsentanten** z_1 *und* z_2.

Beweis: Seien $z_1 = q_1 n + r_1$ und $z_1' = q_1' n + r_1$ zwei Repräsentanten der ersten Restklasse mit $q_1, q_1' \in \mathbb{Z}$ und $0 \leq r_1 < n$.

Ebenso seien $z_2 = q_2 n + r_2$ und $z_2' = q_2' n + r_2$ zwei Repräsentanten der zweiten Restklasse mit $q_2, q_2' \in \mathbb{Z}$ und $0 \leq r_2 < n$.

Dann gilt $\bar{z}_1 = \bar{z}_1' = \bar{r}_1$ und $\bar{z}_2 = \bar{z}_2' = \bar{r}_2$.

Wegen $z_1 + z_2 = (q_1 + q_2)\, n + (r_1 + r_2)$ folgt $\overline{z_1 + z_2} = \overline{r_1 + r_2}$.

Genauso folgt $\overline{z_1' + z_2'} = \overline{r_1 + r_2}$, also insgesamt $\overline{z_1 + z_2} = \overline{z_1' + z_2'}$.

□

Satz (Multiplikation von Restklassen)

Sei $n \in \mathbb{N}_+$ und seinen $\bar{z}_1, \bar{z}_2 \in \mathbb{Z}/n\mathbb{Z}$ zwei Restklassen modulo n, wobei $z_1, z_2 \in \mathbb{Z}$ Repräsentaten dieser Restklassen sind. Dann setzen wir

$$\bar{z}_1 \cdot \bar{z}_2 \;=\; \overline{z_1 \cdot z_2}.$$

Dies ist wohldefiniert und es gelten die üblichen Rechenregeln (Assoziativgesetz, Distributivgesetz, Kommutativgesetz).

Beweis: Schreibe $z_1 = q_1\, n + r_1$ sowie $z_2 = q_2\, n + r_2$ mit $q_1, q_2 \in \mathbb{Z}$ und $r_1, r_2 \in \{0, \ldots, n-1\}$. Dann gilt:

$$z_1 \cdot z_2 = (q_1\, n + r_1)\,(q_2\, n + r_2) = (q_1 q_2 n + q_1 r_2 + q_2 r_1)\, n + r_1 r_2$$

Hieraus folgt, dass $\overline{z_1 \cdot z_2} \;=\; \overline{r_1 r_2}$ nicht von der speziellen Wahl der Repräsentaten z_1, z_2 abhängt. □

Modulare Zahlen

In der Sprache der Algebra ist $\mathbb{Z}/n\mathbb{Z} \quad = \quad \{\ \bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\ \}$ ein **kommutativer Ring**. Er heißt der Ring der **modularen Zahlen** modulo n oder der **Restklassenring** von $\mathbb{Z}$ modulo n.

Das Rechnen in den Ringen $\mathbb{Z}/n\mathbb{Z}$ heißt auch die **Modulorechnung**.

Beispiel

(a) In $\mathbb{Z}/4\mathbb{Z}$ gilt $\bar{0}\cdot\bar{2}=\bar{0}$, $\bar{1}\cdot\bar{2}=\bar{2}$, $\bar{2}\cdot\bar{2}=\bar{0}$ und $\bar{3}\cdot\bar{2}=\bar{2}$.

(b) In $\mathbb{Z}/10\mathbb{Z}$ ist $\bar{z}_1\cdot\bar{z}_2$ die Restklasse der Endziffer von z_1z_2.

Frage: Kann man in $\mathbb{Z}/n\mathbb{Z}$ auch dividieren?

I.A. geht dies nicht, z.B. gibt es in $\mathbb{Z}/4\mathbb{Z}$ kein $\bar{z}$ mit $\bar{z}\cdot\bar{2}=\bar{1}$.

ggT und kgV

Definition

(a) Zu zwei Zahlen $z_1, z_2 \in \mathbb{Z}$ mit $(z_1, z_2) \neq (0, 0)$ heißt die größte ganze Zahl g mit $g \mid z_1$ und $g \mid z_2$ der **größte gemeinsame Teiler (ggT)** von z_1 und z_2. Wir schreiben $\mathrm{ggT}(z_1, z_2)$ und setzen $\mathrm{ggT}(0, 0) = 0$.

(b) Analog definieren wir $\mathrm{kgV}(z_1, z_2)$ als das positive **kleinste gemeinsame Vielfache** von z_1 und z_2.

(c) Zwei Zahlen z_1, z_2 heißen **teilerfremd**, wenn $\mathrm{ggT}(z_1, z_2) = 1$ gilt.

Beispiel

(a) $\mathrm{ggT}(64, 81) = 1$, d.h. $64 = 2^6$ und $81 = 3^4$ sind teilerfremd.

(b) $\mathrm{ggT}(343, 1001) = 7$, denn $343 = 7^3$ und $1001 = 7 \cdot 11 \cdot 13$.

Der erweiterte euklidische Algorithmus

Ziel: Zu zwei Zahlen $z_1, z_2 \in \mathbb{Z}$ berechne ein Tripel $(a, b, c) \in \mathbb{Z}^3$ mit $c = \mathrm{ggT}(z_1, z_2)$ und einer Darstellung $\mathrm{ggT}(z_1, z_2) = a\, z_1 + b\, z_2$.

(1) Im Fall $(z_1, z_2)=(0, 0)$ gib $(0, 0, 0)$ aus. Im Fall $z_1=0$, $z_2\neq 0$ gib $(0, \mathrm{sign}(z_2), |z_2|)$ aus. Im Fall $z_1\neq 0$, $z_2=0$ gib $(\mathrm{sign}(z_1), 0, |z_1|)$ aus.

(2) Bilde die Tripel $(a_0, b_0, c_0) = (\mathrm{sign}(z_1), 0, |z_1|)$ und $(a_1, b_1, c_1) = (0, \mathrm{sign}(z_2), |z_2|)$. Gilt $c_0 < c_1$ so vertausche die beiden Tripel.

(3) Schreibe $c_0 = qc_1 + r$ mit $q \in \mathbb{N}$ und $0 \leq r < c_1$. Bilde dann $(a_2, b_2, c_2) = (a_0 - qa_1, b_0 - qb_1, r)$.

(4) Ersetze $(a_0, b_0, c_0) \leftarrow (a_1, b_1, c_1)$ und $(a_1, b_1, c_1) \leftarrow (a_2, b_2, c_2)$.

(5) Wiederhole **(3)** und **(4)** bis $c_1 = 0$ gilt. Gib dann (a_0, b_0, c_0) aus.

Beweis: Der Algorithmus ist **endlich**, da c_1 bei jedem Schritt kleiner wird. Er ist **korrekt**, weil jederzeit $a_i\, z_1 + b_i\, z_2 = c_i$ gilt. Die Bedingung $c_1 = 0$ am Ende bedeutet, dass einen Schritt vorher c_0 durch c_1 teilbar war. □

Korollar

Sind $z \in \mathbb{Z}$ und $n \in \mathbb{N}_+$ teilerfremd, so berechne $a, b \in \mathbb{Z}$ mit $a\, z + b\, n = 1$. Dann gilt $\bar{z}^{\,-1} = \bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

Beweis: In $\mathbb{Z}/n\mathbb{Z}$ gilt $\bar{a} \cdot \bar{z} + \bar{b} \cdot \bar{0} = \bar{1}$, also $\bar{a} \cdot \bar{z} = \bar{1}$. □

Korollar

*Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein **Körper**, d.h. man kann durch alle Elemente $\neq \bar{0}$ teilen.*

Beweis: Die Zahlen $1, 2, \ldots, p-1$ sind alle teilerfremd zu p. □

Beispiel

Berechne 33^{-1} in $\mathbb{Z}/101\mathbb{Z}$ mittels $a \cdot 101 + b \cdot 33 = 1$.

(2) $(a_0, b_0, c_0) = (1, 0, 101)$ und $(a_1, b_1, c_1) = (0, 1, 33)$.

(3) $101 = 3 \cdot 33 + 2$, also $(a_2, b_2, c_2) = (1, -3, 2)$.

(4) $(a_0, b_0, c_0) = (0, 1, 33)$ und $(a_1, b_1, c_1) = (1, -3, 2)$.

(3) $33 = 16 \cdot 2 + 1$ und $(a_2, b_2, c_2) = (-16, 49, 1)$.

(4) $(a_0, b_0, c_0) = (1, -3, 2)$ und $(a_1, b_1, c_1) = (-16, 49, 1)$.

(3) $2 = 2 \cdot 1 + 0$ und $(a_2, b_2, c_2) = (33, -101, 0)$.

Also folgt $-16 \cdot 101 + 49 \cdot 33 = 1$ und $\overline{33}^{-1} = \overline{49}$.

Frage: Für welche Zahlen $z_1, z_2 \in \{1, 2, \ldots, 100\}$ braucht der euklidische Algorithmus die meisten Schritte?

Antwort: 55 und **89**, also für aufeinanderfolgende **Fibonacci-Zahlen**.

Komplexität: Man braucht maximal $O(\ln(n))$ Divisionen mit Rest.

§2. Der chinesische Restsatz

Gib einem Mann einen Fisch und er hat einen Tag zu essen.

Lehre ihn fischen und er hat ein Leben lang zu essen.

(Konfuzius, 551-479 v.Chr.)

. . . and he sits in a boat and drinks beer all day.

Meister Sun schrieb im 4. Jahrhundert n. Chr. das

Sun Zi Suan Jing

also **Meister Suns Rechenhandbuch**. Es hat 3 Kapitel und enthält in den letzten beiden 28 bzw. 36 Aufgaben.

Aufgabe 26 in Kapitel 3 lautet wie folgt.

Aufgabe. *Gegeben sei eine unbekannte Zahl von Dingen. Zählt man jeweils 3 ab, bleibt ein Rest von 2. Werden jeweils 5 abgezählt, bleibt ein Rest von 3, und bei jeweils 7 ein Rest von 2. Finde die Zahl der Dinge.*

Lösung. Gesucht ist eine Lösung z der **simultanen Kongruenzen**

$$\begin{aligned} z &\equiv 2 \pmod 3 \\ z &\equiv 3 \pmod 5 \\ z &\equiv 2 \pmod 7 \end{aligned}$$

Setze $r_1 = 2$, $n_1 = 3$, $r_2 = 3$, $n_2 = 5$, $r_3 = 2$ und $n_3 = 7$.

Dann verwendet Meister Sun folgende Lösungsformel:

$$\begin{aligned} z &= 70 \cdot r_1 + 21 \cdot r_2 + 15 \cdot r_3 - p \cdot \mathrm{kgV}(3,5,7) \\ &= 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 - 2 \cdot 105 \;=\; 23 \end{aligned}$$

Dabei ist $70 \equiv 0 \pmod{n_2 n_3}$ und $70 \equiv 1 \pmod{3}$, etc., und die Zahl $p = 2$ ist *passend* gewählt.

Nicht unter allen Personen ist eine 3 mal 20 plus 10 Jahre alt,
auf 5 Pflaumenbäumen bleiben nur 21 Zweige übrig,
alle 15 Tage begegnen sich die 7 Gelehrten,
unsere Lösung erhalten wir, wenn wir mehrfach 105 abziehen.
(altes chinesisches Volkslied **Sun Zi Ge** (Meister Suns Lied))

Satz (Zwei simultane Kongruenzen)

Seien $n_1, n_2 \in \mathbb{N}_+$ teilerfremde Zahlen und seien $a_1, a_2 \in \mathbb{Z}$. Gesucht seien alle Lösungen x des Systems simultaner Kongruenzen

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

(a) *Mit dem erweiterten euklidischen Algorithmus berechne $b_1, b_2 \in \mathbb{Z}$ mit $b_1\, n_1 + b_2\, n_2 = 1$. Dann ist $x = a_2\, b_1\, n_1 + a_1\, b_2\, n_2$ eine Lösung des Systems.*

(b) *Ist $y \in \mathbb{Z}$ eine weitere Lösung des Systems, so ist y von der Form $y = x + c\, n_1\, n_2$ mit $c \in \mathbb{Z}$.*

Beweis: **"(a)"** $x \equiv a_i b_{3-i} n_{3-i} \equiv a_i \pmod{n_i}$, da $b_{3-i} n_{3-i} \equiv 1 \pmod{n_i}$. **"(b)"** $y - x$ ist durch n_1 und n_2, also durch $\mathrm{kgV}(n_1, n_2) = n_1\, n_2$ teilbar. □

Satz (Der chinesische Restsatz)

Seien $n_1, \ldots, n_k \in \mathbb{N}_+$ *paarweise teilerfremd und* $a_1, \ldots, a_k \in \mathbb{Z}$.

Dann besitzt das System der simultanen Kongruenzen

$x \equiv a_1 \pmod{n_1}, \ \ldots, \ x \equiv a_k \pmod{n_k}$ *eine Lösung* $x \in \mathbb{Z}$ *und die*

Menge aller Lösungen ist sodann $\mathbb{L} = \{x + c\, n_1 \cdots n_k \mid c \in \mathbb{Z}\}$.

Beweis: Verwende den letzten Satz für (n_1, n_2), dann für $(n_1 n_2, n_3)$ etc. □

Bemerkung

Die algebraische Formulierung dieses Satzes ist, dass die Abbildung

$\varphi : \ \mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z} \ \longrightarrow \ (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$

mit $\varphi(x + n_1 \cdots n_k\mathbb{Z}) = (x + n_1\mathbb{Z}, \ldots, x + n_k\mathbb{Z})$ ein Isomorphismus von Ringen ist.

§3. Der kleine Satz von Fermat

Seit man begonnen hat,
die einfachsten Behauptungen zu beweisen,
erwiesen sich viele von ihnen als falsch.
(Bertrand Russell)

Obwohl **Pierre de Fermat** (1607-1665) behauptete, alle seine zahlentheoretischen Sätze bewiesen zu haben, sind kaum Beweise von ihm überliefert. Auch für den nach ihm benannten "kleinen Satz von Fermat" findet sich der erste veröffentlichte Beweis bei Euler (1741).

Satz (Kleiner Satz von Fermat)

Ist p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$, so gilt $a^{p-1} \equiv 1 \pmod{p}$.

Beweis: Subtrahieren wir von a ein Vielfaches von p, so bleibt $a^{p-1} \pmod p$ unverändert. Also können wir $1 \leq a \leq p-1$ annehmen.

Betrachte nun die Reste von a, $2a$, $\ldots$, $(p-1)\,a$ modulo p. Dies sind $p-1$ verschiedene Zahlen in $\{1, \ldots, p-1\}$, denn wären zwei gleich, z.B. $i\,a \equiv j\,a \pmod p$, so würde p das Produkt $(i-j)\,a$ teilen. Nach dem Satz von Euklid würde p dann a oder $(i-j)$ teilen, was nicht geht, da beide Zahlen kleiner als p sind.

Somit sind diese Reste eine Permutation der Zahlen $1, \ldots, p-1$. Also ist ihr Produkt $1 \cdot 2 \cdots (p-1) = (p-1)!$, d.h. es gilt

$$a \cdot (2a) \cdots (p-1)a = (p-1)!\; a^{p-1} \equiv (p-1)! \pmod p$$

Da $(p-1)!$ teilerfremd ist zu p, dürfen wir es in $\mathbb{Z}/p\mathbb{Z}$ kürzen. Folglich besitzt a^{p-1} den Rest 1 modulo p. □

Laut der Modulbeschreibung für **Zahlentheorie und Kryptologie** sollen die Schüler den kleinen Satz von Fermat beweisen können.

Beispiel

Bestimme $1001^{1001} \pmod{101}$.

Nach dem kleinen Satz von Fermat gilt $1001^{100} \equiv 1 \pmod{101}$, da 101 eine Primzahl ist, die 1001 nicht teilt. Also folgt:

$$1001^{1001} = (1001^{100})^{10} \cdot 1001 \equiv 1001 \equiv \mathbf{92} \pmod{101}.$$

Korollar

Ist p eine Primzahl und $a \in \mathbb{Z}$, so gilt $a^p \equiv a \pmod{p}$.

Beweis: Im Fall $p \nmid a$ multipliziere den kleinen Satz von Fermat mit a. Im Fall $p \mid a$ steht hier $0 \equiv 0 \pmod{p}$. □

Bemerkung (Der Fermat-Primzahltest)

Sei $n \in \mathbb{N}_+$. Gilt für eine Zahl $a \in \mathbb{Z}$ mit $n \nmid a$ die Bedingung $a^{n-1} \not\equiv 1 \pmod{n}$, so kann n keine Primzahl sein.

Beispiel

(a) Testen wir, ob **341** eine Primzahl ist.

$2^{340} \equiv 1 \pmod{341}$, d.h. 341 könnte eine Primzahl sein.

$3^{340} \equiv 56 \pmod{341}$, also ist 341 keine Primzahl. $(341 = 11 \cdot 31.)$

Die Zahl 341 ist eine **Pseudoprimzahl** zur Basis 2.

(b) Testen wir, ob **561** eine Primzahl ist.

Es stellt sich heraus, dass für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, 561) = 1$ gilt $a^{560} \equiv 1 \pmod{561}$. Wegen $561 = 3 \cdot 11 \cdot 17$ ist 561 eine Pseudoprimzahl zu jeder passenden Basis a, aber keine Primzahl.

Eine solche Zahl heißt eine **Carmichael-Zahl**.

Frage: Wie berechnet man hohe Potenzen modulo n?

Satz (Iteriertes Quadrieren)

Seien $a, k, n \in \mathbb{N}_+$. Berechne $a^k \pmod n$ wie folgt:

(1) *Schreibe k im Binärsystem als $k = c_0 + c_1 \cdot 2 + \cdots + c_\ell \cdot 2^\ell$ mit Ziffern $c_i \in \{0, 1\}$.*

(2) *Sei $b_0 \equiv a \pmod n$ mit $0 \leq b_0 < n$. Berechne $b_1 \equiv b_0^2 \pmod n$ durch Division mit Rest, also mit $0 \leq b_1 < n$. So fortfahrend berechne $b_i \equiv b_{i-1}^2 \pmod n$ mit $0 \leq b_i < n$ für $i = 2, \ldots, \ell$.*

(3) *Nun multipliziere alle $b_i \pmod n$, für die $c_i = 1$ gilt. (Um die Zahlen klein zu halten, kann man nach der Multiplikation mit einem b_i jedes Mal modulo n reduzieren.)*

Das Ergebnis $\prod_{c_i=1} b_i \pmod n$ ist gleich $a^k \pmod n$.

Beweis: $b_i \equiv a^{2^i} \pmod n$ und $a^k = a^{c_0} \cdot a^{c_1 \cdot 2} \cdots a^{c_\ell \cdot 2^\ell} = \prod_{c_i=1} a^{2^i}$.

Beispiel

Die Restklasse $3^{340} \pmod{341}$ soll berechnet werden.

(1) $340 = 256 + 84 = 256 + 64 + 16 + 4$

(2) $3^2 \equiv 9 \pmod{341}$, $3^4 \equiv 9^2 \equiv 81 \pmod{341}$,
$3^8 \equiv 81^2 \equiv 82 \pmod{341}$, $3^{16} \equiv 82^2 \equiv 245 \pmod{341}$,
$3^{32} \equiv 245^2 \equiv 9 \pmod{341}$, $3^{64} \equiv 9^2 \equiv 81 \pmod{341}$,
$3^{128} \equiv 82 \pmod{341}$ und $3^{256} \equiv 245 \pmod{341}$.

(3) $3^{340} = 3^4 \cdot 3^{16} \cdot 3^{64} \cdot 3^{256} \equiv 81 \cdot 245 \cdot 81 \cdot 245 \equiv \mathbf{56} \pmod{341}$

§4. Der Satz von Euler

Das ist Fussball.

Manchmal gewinnt das bessere Team.

(Lukas Podolski)

Frage: Gibt es auch eine Version des kleinen Satzes von Fermat, wenn man modulo n rechnet, aber n keine Primzahl ist?

Definition

Sei $n \in \mathbb{N}_+$. Die Anzahl aller Zahlen in $\{1, 2, \ldots, n\}$, die zu n teilerfremd sind, werde mit $\varphi(n)$ bezeichnet. Die Abbildung $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ heißt die **Eulersche φ-Funktion**.

Beispiel

(a) $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$

(b) $\varphi(p) = p - 1$ für jede Primzahl p

(c) $\varphi(25) = 25 - 5 = 20$

(d) Für eine Primzahl p gilt $\varphi(p^2) = p^2 - p = p(p-1)$.

(e) Für eine Primzahl p und $k \geq 2$ gilt

$$\varphi(p^k) \;=\; p^k - p^{k-1} \;=\; p^{k-1}\,(p-1).$$

Satz

Sind $m, n \in \mathbb{N}_+$ teilerfremde Zahlen, so gilt $\varphi(m\,n) = \varphi(m) \cdot \varphi(n)$.

Beweis: Eine Zahl in $\{1, \ldots, mn\}$ ist genau dann teilerfremd zu mn, wenn sie in $\mathbb{Z}/mn\mathbb{Z}$ invertierbar ist. Nach dem chinesischen Restzsatz gilt dies genau dann, wenn sie in $\mathbb{Z}/m\mathbb{Z}$ und in $\mathbb{Z}/n\mathbb{Z}$ invertierbar ist. Es gibt $\varphi(m) \cdot \varphi(n)$ Paare invertierbarer Restklassen. □

Beispiel

Es gilt $\varphi(1000) = \varphi(2^3) \cdot \varphi(5^3) = 2^2 \cdot 1 \cdot 5^2 \cdot 4 = 400$.

Satz (Der Satz von Euler)

Sei $n \in \mathbb{N}_+$ und sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Beweis: Seien $r_1, \ldots, r_{\varphi(n)} \in \{1, \ldots, n\}$ die zu n teilerfremden Zahlen. Dann sind auch $ar_1, \ldots, ar_{\varphi(n)}$ zu n teilerfremd. Die Restklassen modulo n dieser Zahlen sind paarweise verschieden, denn aus $ar_i \equiv ar_j \pmod{n}$ folgt $r_i \equiv r_j \pmod{n}$.

Somit ist $(\bar{a}\bar{r}_1, \ldots, \bar{a}\bar{r}_{\varphi(n)})$ eine Permutation von $(\bar{r}_1, \ldots, \bar{r}_{\varphi(n)})$ und

$r_1 \cdots r_{\varphi(n)} \equiv (a\, r_1) \cdots (a\, r_{\varphi(n)}) \equiv a^{\varphi(n)} \cdot (r_1 \cdots r_{\varphi(n)}) \pmod{n}$.

Da man durch die r_i modulo n kürzen darf, folgt $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Beispiel

Finde die letzten drei Ziffern von 2^{2023}.

Gesucht ist also die Restklasse von 2^{2023} modulo 1000. Wegen $\varphi(1000) = 400$ liefert der Satz von Euler $2^{2023} \equiv 2^{23} \pmod{1000}$.
Mit $2^{10} = 1024$ folgt $2^{23} \equiv 24^2 \cdot 8 \equiv 576 \cdot 8 \equiv \mathbf{608} \pmod{1000}$.

Korollar

Ist $n = pq$ das Produkt zweier Primzahlen p, q, so gilt $\varphi(n) = (p-1)(q-1)$ und für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ folgt $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$.

§5. Fortgeschrittene Resterechnung

Jeder ist ein Ignorant.

Aber halt auf verschiedenen Gebieten.

(Will Rogers)

Definition. Sei $n \in \mathbb{N}_+$. Eine Zahl $a \in \{1, \ldots, n-1\}$ heißt ein **quadratischer Rest** modulo n, wenn sie zu n teilerfremd ist und die Gleichung $x^2 \equiv a \pmod{n}$ eine Lösung besitzt.

Beispiel. Modulo $n = 3$ gibt es nur den quadratischen Rest 1, denn $\bar{1}^2 = \bar{2}^2 = \bar{1}$. Die **Quadrate** in $\mathbb{Z}/3\mathbb{Z}$ sind also $\bar{0}$ und $\bar{1}$.

Satz

Sei $p \geq 3$ eine ungerade Primzahl. Von den $p-1$ Restklassen $\bar{1}, \ldots, \overline{p-1}$ in $\mathbb{Z}/p\mathbb{Z}$ sind genau die Hälfte quadratische Reste.

Beweis: Die Reste $\bar{i}$ und $\overline{p-i}$ haben für $i = 1, \ldots, \frac{p-1}{2}$ jeweils das gleiche Quadrat. Ist a ein quadratischer Rest mit $\bar{a} = \bar{b}^2$, so hat die Gleichung $x^2 - \bar{a} = 0$ wegen $x^2 - \bar{b}^2 = (x - \bar{b})(x + \bar{b}) = 0$ in dem Körper $\mathbb{Z}/p\mathbb{Z}$ genau zwei Lösungen. (Ist in einem Körper ein Produkt von zwei Elementen gleich null, so ist eines davon schon null.) □

Beispiel

Hat $5x^2 - 6y^2 = 7$ eine Lösung mit $x, y \in \mathbb{Z}$?

Modulo 5 lautet diese Gleichung $-y^2 \equiv 2 \pmod 5$, also $y^2 \equiv 3 \pmod 5$. Die Quadrate modulo 5 sind aber $\bar{0}$, $\bar{1}$ und $\bar{4}$. Also hat die Gleichung keine Lösung modulo 5 und somit auch nicht in $\mathbb{Z}$.

Beispiel

(a) Besitzt die Gleichung $x^2 + 91y = 5$ eine Lösung mit $x, y \in \mathbb{Z}$?

Wegen $91 = 7 \cdot 13$ liegt es nahe, die Gleichung modulo 7 zu betrachten, was $x^2 \equiv 5 \pmod 7$ liefert.
Die quadratischen Rest modulo 7 sind $\bar{1}$, $\bar{2}$ und $\bar{4}$. Also besitzt die Gleichung keine Lösungen modulo 7 und somit auch nicht in $\mathbb{Z}$.

(b) Besitzt die Gleichung $x^2 + 91y = 11$ eine Lösung mit $x, y \in \mathbb{Z}$?

Diesmal ist modulo 7 alles OK, aber modulo 13 sind die quadratischen Reste $1, 3, 4, 9, 10, 12$, aber nicht 11.

Satz (Wurzel ziehen modulo p)

Sei p eine Primzahl und $a \in \{1, \ldots, p-1\}$.

(a) *Genau dann ist a ein quadratischer Rest modulo p, wenn $a^{(p-1)/2} \equiv 1 \pmod{p}$ gilt.*

(b) *Ist $p \equiv 3 \pmod{4}$ und a ein quadratischer Rest modulo p, so ist $b \equiv a^{(p+1)/4} \pmod{p}$ eine* **Quadratwurzel** *modulo p aus a.*

Beweis: "(a)" Wegen $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ gilt $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Gilt $a \equiv b^2 \pmod{p}$ so folgt $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$, d.h. quadratische Reste liefern $+1$.

Da die Gleichung $x^{(p-1)/2} - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ höchstens $(p-1)/2$ Lösungen hat, sind dies genau die quadratischen Reste modulo p.

"(b)" folgt aus $b^2 \equiv a^{(p+1)/2} \equiv a^{(p+1)/2} \cdot a^{(p-1)/2} \equiv a^p \equiv a \pmod{p}$.

□

Ich habe fertig.

Ein Mathematiker ist eine Maschine,
die Kaffee in Sätze verwandelt.
(Alfred Renyi)

Vielen Dank für Ihre Aufmerksamkeit!