Korrespondenzzirkel der LSGM 2013/14

Klasse 7, Treff 2 am 22. März 2014

Wir wiederholten die Ergebnisse des 1. Treffens: Permutationen mit und ohne Wiederholung, Teilbarkeitsregeln, Anzahl der Teiler einer Zahl, Potenzgesetz $(a^m)^n = a^{mn}$.

Rechnen mit Kongruenzen

Motivation

Mittels Kongruenzrechnung lassen sich viele zahlentheoretische Aufgaben elegant und einfach lösen.

1. Diophantische Gleichungen (Gleichungen, wo die gesuchten Variablen *ganze* Zahlen sind), wie $15x + 3y = 100$ oder $24x + 36y = 3334$ oder $x^2 = 8y + 7$ oder $x^2 + y^2 + z^2 = 8u + 7$.
2. Teilbarkeitsregeln $n \equiv Q(n) \pmod 9$, $n \equiv A(n) \pmod{11}$.
3. Auf welche beiden Ziffern endet 7^{7^7}?
4. Beweise: Für alle natürlichen Zahlen $m, n \in \mathbb{N}$ gilt $44 \mid 43^{2n+1} + 87^{2m}$.
5. Wie lautet die letzte Ziffer von f_{2014}, wenn $(f_n) = (1, 1, 2, 3, 5, 8, 13, 21, \dots)$ die Fibonacci-Folge ist?

Zahlenkongruenzen — Modulorechnung

Welche Reste treten bei Division durch 3 auf, natürlich 0, 1 und 2. Alle ganzen Zahlen, die denselben Rest lassen fassen wir zu einer *Restklasse* zusammen:

$$[0]_3 = \{0, 3, 6, 9, -3, -6, -9, -12, \dots\} = \{3n \mid n \in \mathbb{Z}\},$$
$$[1]_3 = \{1, 4, 7, 10, 13, -2, -5, -8, \dots\} = \{3n + 1 \mid n \in \mathbb{Z}\},$$
$$[2]_3 = \{2, 5, 8, 11, -1, -4, -7, \dots\} = \{3n + 2 \mid n \in \mathbb{Z}\}.$$

Zahlen, die in derselben Klasse liegen heißen *zueinander kongruent modulo 3*. Wir schreiben

$$0 \equiv 3 \pmod 3, \quad 7 \equiv -8 \pmod 3, \quad 5 \equiv -7 \pmod 3.$$

Bei der Division durch 2 gibt es nur zwei Restklassen, 0 und 1. Die Restklasse $[0]_2$ der durch 2 teilbaren Zahlen ist die Menge der geraden Zahlen und die Restklasse $[1]_2$ ist die Menge

der ungeraden Zahlen. Die Kongruenz modulo m ist eine *Äquivalenzrelation* auf der Menge der ganzen Zahlen: Jede ganze Zahl liegt in einer Äquivalenzklasse und keine ganze Zahl liegt in mehreren Äquivalenzklassen. Die Haupteigenschaften einer Äquivalenzrelation sind *Reflexivität*, *Symmetrie* und *Transitivität*.

Nun kann man an Stelle von 2 oder 3 einen beliebigen *Modul* $m \in \mathbb{N}$, $m \geq 2$ betrachten. Das führt zu folgender allgemeinen Definition:

Definition 1 Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* m, wenn eine der folgenden vier zueinander äquivalenten Bedingungen erfüllt ist:

1. a und b lassen bei Division durch m denselben Rest.
2. $m \mid (a-b)$, m teilt die Differenz der beiden Zahlen.
3. $\frac{a-b}{m} \in \mathbb{Z}$. Der Quotient ist eine ganze Zahl.
4. $\exists q \in \mathbb{Z}: a = qm + b$.

Wir schreiben $a \equiv b \pmod{m}$ und sprechen „a ist kongruent b modulo m“.

Spezialfall: $b = 0$. $a \equiv 0 \pmod{m}$ bedeutet nach Bedingung 2. $m \mid a$.

Beispiele:

$$12345 \equiv 54321 \pmod 3, \quad 91 \equiv 35 \pmod 7, \quad 123456 \equiv 6 \pmod{10}, \quad 123456 \equiv 56 \pmod{100},$$
$$2010 \equiv -3 \pmod{11}, \quad 2011 \equiv 1 \pmod 3.$$

Spezialfälle: $m = 10$ und $m = 100$. Zwei (natürliche) Dezimalzahlen sind kongruent modulo 10, wenn sie auf dieselbe Ziffer enden. Zwei Dezimalzahlen sind kongruent modulo 100, wenn ihre letzten beiden Ziffern übereinstimmen.

Wir erwähnen drei weitere Spezialfälle: Die Teilbarkeitsregeln für 9, 3 und 11. Bezeichnet man mit $Q(n)$ die Quersumme einer natürlichen Zahl n und mit $A(n)$ deren alternierende Quersumme, begonnen mit der Einerziffer: $A(123456) = 6-5+4-3+2-1 = 3$, $Q(123456) = 1+2+3+4+5+6 = 21$, dann gilt

$$n \equiv Q(n) \pmod 9, \quad n \equiv Q(n) \pmod 3, \quad n \equiv A(n) \pmod{11}.$$

Beispiel:

$$12345678910 \equiv Q(12345678910) \equiv 1+2+3+\cdots+10 \equiv 55 \equiv Q(55) \equiv 10 \equiv Q(10) \equiv 1 \pmod{10}.$$

$$5^n \equiv 5 \pmod{10}, \quad 6^n \equiv 6 \pmod{10}, \quad 1^n \equiv 1 \pmod{10}, \quad 0^n \equiv 0 \pmod{10}$$
$$4^n \equiv 4,6 \pmod{10}, \quad 9^n \equiv 9,1 \pmod{10}$$
$$2^n \equiv 2,4,8,6 \pmod{10}, \quad 3^n \equiv 3,9,7,1 \pmod{10}, \quad 7^n \equiv 7,9,3,1 \pmod{10}$$

Es gilt der *Kleine Fermatsche Satz*: Für jede Primzahl p und jede natürliche Zahl a, die nicht durch p teilbar ist gilt $a^{p-1} \equiv 1 \pmod p$. Dabei ist $p-1$ nicht notwendig die kleinste Periode von $(a^n \pmod p)$, doch die Periode ist ein Teiler von $p-1$. So hat $2^n \pmod 7$ die Periode 3, denn $2^3 \equiv 1 \pmod 7$.

Eigenschaften der Kongruenzen

Reflexivität, Symmetrie und Transitivität: Für alle ganzen Zahlen $a, b, c \in \mathbb{Z}$ gilt:

$$\begin{aligned}
&a \equiv a \pmod{m},\\
&a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m},\\
&a \equiv b \pmod{m}, \quad b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}.
\end{aligned}$$

Rechnen mit Kongruenzen

Kongruenzen können wie Gleichungen addiert, subtrahiert, multipliziert und potenziert-werden. Genauer, wenn $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, dann gilt auch

$$\begin{aligned}
a + c &\equiv b + d \pmod{m}\\
a - c &\equiv b - d \pmod{m}\\
ac &\equiv bd \pmod{m}\\
a^n &\equiv b^n \pmod{m}
\end{aligned}$$

Hierbei ist n eine beliebige natürliche Zahl.

Die Division kommt später.

Wir beweisen die Neuner- und die Elferregel anhand von 4-stelligen Zahlen im Dezimalsystem $n = 1000a + 100b + 10c + d$, $Q(n) = a + b + c + d$, $A(n) = d - c + b - a$. Wir berechnen

1) $123 \cdot 456 \cdot 789 \pmod 9$.
2) $2^{100} \pmod 7$. Hinweis: Bestimme zunächst die Reste von $2^0, 2^1, 2^2, 2^3, 2^4, \ldots$ und versuche eine Regelmäßigkeit festzustellen.
3) $44^{44} \cdot 55^{55} \cdot 66^{66} \pmod{10}$
4) $87^{432} + 45^{17} \pmod{11}$

Wir beweisen, dass $x^2 + y^2 + z^2 = 8u + 7$ in ganzen Zahlen keine Lösung hat. Denn es gilt modulo 8:

$$x \equiv \begin{cases} 0 \\ \pm 1 \\ \pm 2 \\ \pm 3 \\ 4 \end{cases} \pmod 8, \quad x^2 \equiv \begin{cases} 0 \\ 1 \\ 4 \\ 1 \\ 0 \end{cases} \pmod 8$$

Dieselben Reste können für y^2 und z^2 auftreten. Addiert beliebige drei dieser Reste 0, 1 oder 4, so gibt es 10 Fälle: $0 + 0 + 0 = 0$, $0 + 0 + 1 = 1$, ... In keinem dieser Fälle erhält man als Summe 7 (mod 8). Wir zeigen $x^2 + y^2 \equiv 3 \pmod 4$ hat keine Lösung.

Pause: Rasende Roboter.