TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften, Fakultät Mathematik, Institut für Algebra

Jun.-Prof. Friedrich Martin Schneider, Dr. Henri Mühle. Wintersemester 2018/19

9. Übungsblatt zur Vorlesung "Diskrete Strukturen für Informatiker"

Modulare Arithmetik

V. Die *Dezimaldarstellung* von $n \in \mathbb{N}$ ist das eindeutig bestimmte Tupel $(n_0, n_1, \ldots, n_k)$, mit $0 \leq n_i \leq 9$ für alle i, sodass $n = \sum_{i=0}^{k} n_i 10^i$ und $n_k \neq 0$ gilt. Die *alternierende Quersumme* von n ist dann $\mathrm{aq}(n) = \sum_{i=0}^{k} (-1)^i n_i$.

(a) Bestimmen Sie $\mathrm{aq}(924)$ und $\mathrm{aq}(2143)$.

(b) Zeigen Sie, dass n genau dann durch elf teilbar ist, wenn $\mathrm{aq}(n)$ durch elf teilbar ist.

Ü49. (a) Berechnen Sie für die folgenden Elemente $x \in \mathbb{Z}_n$ jeweils das multiplikative Inverse modulo n, falls es existiert.

(i) $x = 18,\ n = 31,$ (ii) $x = 60,\ n = 257,$
(iii) $x = 511,\ n = 1001,$ (iv) $x = 512,\ n = 1001.$

(b) Geben Sie die Lösungsmengen der folgenden Kongruenzen an.

(i) $5x \equiv 1 \pmod 7$, (ii) $32x \equiv 14 \pmod{82}$, (iii) $10x \equiv 9 \pmod{25}$.

Hinweis: Es gibt eine Regel zur Modulo-Rechnung, mit deren Hilfe die Kongruenz in (ii) geeignet umgeformt werden kann.

Ü50. Seien $a, b, n \in \mathbb{N}$. Um $a^b \pmod n$ zu berechnen, bietet sich der folgende *Square-and-Multiply*-Algorithmus an.

> Zuerst berechnet man die *Binärdarstellung* von b, also das eindeutig bestimmte Tupel $(b_0, b_1, \ldots, b_k)$ mit $b_i \in \{0, 1\}$ für alle i, sodass $b = \sum_{i=0}^{k} b_i 2^i$ und $b_k = 1$ gilt. Anschließend initialisiert man $c_{k+1} = 1$ und führt für i von k bis 0 (absteigend) die Rekursion $c_i = c_{i+1}^2 a^{b_i} \pmod n$ aus. Der letzte berechnete Wert c_0 erfüllt dann $c_0 \equiv a^b \pmod n$.

(a) Berechnen Sie mit Hilfe dieses Algorithmus die folgenden Potenzen.

(i) $11^{53} \pmod 8$, (ii) $7^{199} \pmod{11}$, (iii) $37^{25} \pmod{19}$.

(b) Bestimmen Sie die letzten beiden Ziffern von 2^{333}.

sei $x \in \mathbb{Z}_n$. $ggT(x,n)=1 \Rightarrow x$ invertierbar.

I: $x=18$
$n=31$

	31	1	0
-1	18	0	1
-1	13	1	-1
-2	5	-1	2
-1	3	3	-5
-1	2	-4	7
-2	1	7	-12
	0		

$ggT(18,31)=1=7\cdot 31-12\cdot 18$

$1 \equiv 7\cdot 31 - 12\cdot 18 \pmod{31}$

$1 \equiv -12\cdot 18 = -216 = (-7)\cdot 31+1$

$1 \equiv 19\cdot 18 = 342 = 11\cdot 31+1$

ii: $x=60$
$n=257$

	257	1	0
-4	60	0	1
-3	17	1	-4
-1	9	-3	13
-1	8	4	-17
-8	1	-7	30
	0		

$ggT(60,257) = -7\cdot 257 + 30\cdot 60 = 1$

$1 \equiv -7\cdot 257 + 30\cdot 60 \pmod{257}$

$1 \equiv 30\cdot 60 \pmod{257}$

iii) $x=511$
$n=1001$

	1001	1	0
-1	511	0	1
-1	490	1	-1
-23	21	-1	2
-3	7	24	-47
	0		

$ggT(511,1001)=7=24\cdot 1001 - 47\cdot 511$

b) $5x \equiv 1 \pmod 7 \quad |\cdot 3$

$3\cdot 5x \equiv 3\cdot 1 \ (2)$

$15x \equiv 3 \ (6)$

$x \equiv 3 \ (6)$

$L = \{3n \mid n \in \mathbb{Z}\}$
$= \{n \in \mathbb{Z} \mid 3 \mid n\}$

ii) $32x \equiv 14 \pmod{82}$
$\Leftrightarrow 16x \equiv 7 \pmod{41}$

$18\cdot 16x \equiv 7\cdot 18$

$x \equiv 126$

$x \equiv 3$

iii) $10x \equiv 9 \pmod{25}$

$ggT(10,25)=5 \nmid 9$

keine Lösung

$11^{53} \equiv 3^{53} \pmod 8$ $\quad 53 = [110101]_2$

$53 = (((1\cdot 2+1)\cdot 2\cdot 2+1)\cdot 2\cdot 2+1)$

$3^{53} \equiv 3^{1+2\cdot 2\cdot(1+2\cdot 2(1+2))}$

$\equiv 3^1 \, 3^{2\cdot 2\cdot(1+2\cdot 2(1+2))} \pmod 8$

$\equiv 3\cdot 9^{2\cdot(1+2\cdot 2(1+2))}$ $\quad (\cdot 1)$

$\equiv 3\cdot 1^{2\cdot(1+2\cdot 2(1+2))}$ $\quad (\cdot 1)$

$\equiv 3$

i	
1	0
1	1
1	0
1	0
1	0
1	0
1	0

b) $2^{333} \equiv \quad \pmod{100}$

(5) $P \in \mathbb{P}$ $\quad \mathbb{Z}_p$ $\quad \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

$|\mathbb{Z}_n^*| = \varphi(n)$

$|\mathbb{Z}_p^*| = p-1$

$\mathbb{Z}_{11}$

i	2^i	3^i	6^i
1	2	3	6
2	4	9	3
3	8	5	7
4	5	4	9
5	10	1	10
6	9	3	5
7	7	9	8
8	3	5	4
9	6	4	2
10	1	1	1

$2^{35} - 2^{21} \equiv 2^{10}\cdot 2^{10}\cdot 2^{10}\cdot 2^5 - 2^{21} \pmod{10}$

$\equiv 2^5 - 2^1 \pmod{10}$

$\equiv 10 - 2 \equiv 8$

ii) $\frac{1}{6^5} \equiv 6^{-5} \equiv 6^{10}\cdot 6^{-5} \pmod{11}$

$\equiv 6^5 \equiv 10$

Ü51. Es sei $p \in \mathbb{N}$ eine Primzahl. Die *Logarithmentafel* zu $x \in \mathbb{Z}_p$ ist die Tabelle, die für $i \in \{1, 2, \ldots, p-1\}$ in der i-ten Zeile die Werte i und $x^i \pmod p$ enthält. Die Zahl x ist *primitiv*, wenn $x^i \not\equiv 1 \pmod p$ für alle $i \in \{1, 2, \ldots, p-2\}$ gilt.

(a) Stellen Sie für 2, 3, und 6 die Logarithmentafeln in $\mathbb{Z}_{11}$ auf, und schlussfolgern Sie, welche dieser Zahlen primitiv sind.

(b) Berechnen Sie unter Ausnutzung der Ergebnisse aus (a) die folgenden Werte in $\mathbb{Z}_{11}$.

$$\text{(i)} \quad 2^{35} - 2^{21}, \quad \text{(ii)} \quad \frac{1}{6^5}, \quad \text{(iii)} \quad \frac{3}{7}, \quad \text{(iv)} \quad 17^{457}, \quad \text{(v)} \quad 9^{-1}.$$

A52. **Hausaufgabe, bitte vor Beginn der 10. Übung (oder im Lernraum) unter Angabe von Name, Matrikelnummer, Übungsgruppe und Übungsleiter abgeben.**
Erzeugen Sie erneut mit Hilfe Ihrer Matrikelnummer die Zahlen x und y wie in Aufgabe A40.

(a) Berechnen Sie jeweils das multiplikativ Inverse von x und y modulo 101, falls es existiert.

(b) Berechnen Sie $x^{y \bmod \varphi(101)} \pmod{101}$ mittels Square-and-Multiply.

H53. Wir betrachten den Ring $(\mathbb{Z}_n, +, \cdot)$, wobei Addition und Multiplikation modulo n ausgeführt werden. Eine Zahl $x \in \mathbb{Z} \setminus \{0\}$ ist ein *Nullteiler*, wenn es $y \in \mathbb{Z}_n \setminus \{0\}$ gibt, sodass $x \cdot y \equiv 0 \pmod n$ gilt.

(a) Bestimmen Sie alle Nullteiler und Einheiten in $(\mathbb{Z}_n, +, \cdot)$ für die folgenden Werte von n.

$$\text{(i)} \quad n = 4, \quad \text{(ii)} \quad n = 5, \quad \text{(iii)} \quad n = 15, \quad \text{(iv)} \quad n = 17.$$

(b) Zeigen Sie, dass jedes von Null verschiedene Element in $(\mathbb{Z}_n, +, \cdot)$ entweder eine Einheit oder ein Nullteiler ist.

(c) Zeigen Sie, dass es in $(\mathbb{Z}_n, +, \cdot)$ genau dann keine Nullteiler gibt, wenn $n = 1$ oder n eine Primzahl ist.

H54. (a) Berechnen Sie Lösungen der Kongruenz $225 + 7 \cdot 3^x \equiv 2992 \pmod{13}$.

(b) Zeigen Sie, dass für alle $n \in \mathbb{N}$ die Zahl $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ eine natürliche Zahl ist.