Mathematik: Diskrete Strukturen
Lösungsblatt

Anton Bubnov, Yevgen Kuzmenko

April 28, 2015

Vertiefung:

(a) Bestimmen Sie $\mathrm{mod}(5^{31} \cdot 2^{789} - 23^{23}, 10)$.
Bemerkung 1: die höhere Potenzen werden in Potenzen von 2 ausgeteilt.
Ein Beispiel für 2^{2^n}:

$$\begin{aligned}
&\mathrm{mod}\ (2,10) = 2\\
&\mathrm{mod}\ (2^2,10) = 4\\
&\mathrm{mod}\ (2^4,10) = \mathrm{mod}(2^2 \cdot 2^2, 10) = \mathrm{mod}(\mathrm{mod}(4,10) \cdot \mathrm{mod}(4,10), 10) = \mathrm{mod}(16,10) = 6\\
&\mathrm{mod}\ (2^8,10) = \mathrm{mod}(2^4 \cdot 2^4, 10) = \mathrm{mod}(6 \cdot 6, 10) = 6\\
&\mathrm{mod}\ (2^{16},10) = \mathrm{mod}(2^8 \cdot 2^8, 10) = \mathrm{mod}(6 \cdot 6, 10) = 6\\
&\ldots\\
&\mathrm{mod}\ (2^{512},10) = \mathrm{mod}(2^{256} \cdot 2^{256}, 10) = \mathrm{mod}(6 \cdot 6, 10) = 6
\end{aligned}$$

Also auf solche Weise kann man rekursiv Modulus für Zahlen mit höhe Potenzen berechnen.
Für Modulus Rechenregeln wird Theorem 1.2 (BM) benutzt.

$$\mathrm{mod}(5^{31}, 10) = 5 \qquad (\text{da mod } (5^n, 10) = 5, \forall n \in \mathbb{N}, n \geq 1) \text{ Siehe Bem. 2}$$

$$\begin{aligned}
\mathrm{mod}(2^{789}, 10) &= \mathrm{mod}(2^{512} \cdot 2^{256} \cdot 2^{16} \cdot 2^4 \cdot 2^1, 10)\\
&= \mathrm{mod}(\mathrm{mod}(2^{512},10) \cdot \mathrm{mod}(2^{256},10) \cdot \mathrm{mod}(2^{16},10) \cdot \mathrm{mod}(2^4,10) \cdot \mathrm{mod}(2^1,10), 10)\\
&= \mathrm{mod}(6 \cdot 6 \cdot 6 \cdot 6 \cdot 2, 10)\\
&= \mathrm{mod}(6 \cdot 2, 10)\\
&= 2
\end{aligned}$$

$$\begin{aligned}
\mathrm{mod}(-23^{23}, 10) &= \mathrm{mod}(23^{16} \cdot 23^4 \cdot 23^2 \cdot (-23)^1, 10)\\
&= \mathrm{mod}(\mathrm{mod}(23^{16},10) \cdot \mathrm{mod}(23^4,10) \cdot \mathrm{mod}(23^2,10) \cdot \mathrm{mod}((-23)^1,10), 10)\\
&= \mathrm{mod}(9 \cdot 7, 10) \qquad (\text{da mod } (23^2, 10) = 9 \text{ und mod } (23^4, 10) = 1)\\
&= \mathrm{mod}(63, 10)\\
&= 3
\end{aligned}$$

$$\begin{aligned}
\mathrm{mod}(5^{31} \cdot 2^{789} - 23^{23}, 10) &= \mathrm{mod}(5 \cdot 2 + 3, 10)\\
&= \mathrm{mod}(13, 10)\\
&= 3
\end{aligned}$$

Bemerkung 2: Aussage $\mathrm{mod}(5^n, 10) = 5, \forall n \in \mathbb{N}, n \geq 1$ kann man mit Vollstandige Induktion beweisen:

$$IA : n = 1 : \mathrm{mod}(5^1, 10) = 5$$

$$
\begin{aligned}
IS: \operatorname{mod}(5^{n+1}, 10) &= \operatorname{mod}(\operatorname{mod}(5^n, 10) \cdot \operatorname{mod}(5, 10), 10) \\
&= \operatorname{mod}(5 \cdot 5, 10) \\
&= \operatorname{mod}(25, 10) \\
&= 5
\end{aligned}
$$

(b) Bestimmen Sie $\operatorname{mod}(5^{31} \cdot 2^{789} - 23^{23}, 11)$.

$$
\begin{aligned}
\operatorname{mod}(5^1, 11) &= 5 \\
\operatorname{mod}(5^2, 11) &= \operatorname{mod}(5 \cdot 5, 11) = 3 \\
\operatorname{mod}(5^3, 11) &= \operatorname{mod}(3 \cdot 5, 11) = 4 \\
\operatorname{mod}(5^4, 11) &= \operatorname{mod}(3 \cdot 3, 11) = 9 \\
\operatorname{mod}(5^5, 11) &= \operatorname{mod}(3 \cdot 4, 11) = 1 \\
\operatorname{mod}(5^{31}, 11) &= \operatorname{mod}(\operatorname{mod}(5^5, 11)^6 \cdot \operatorname{mod}(5, 11), 11) \\
&= 5;
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{mod}(2^1, 11) &= 2 \\
\operatorname{mod}(2^2, 11) &= 4 \\
\operatorname{mod}(2^3, 11) &= 8 \\
\operatorname{mod}(2^4, 11) &= 5 \\
\operatorname{mod}(2^5, 11) &= 10 \\
\operatorname{mod}(2^6, 11) &= 9 \\
\operatorname{mod}(2^7, 11) &= 7 \\
\operatorname{mod}(2^8, 11) &= 3 \\
\operatorname{mod}(2^9, 11) &= 6 \\
\operatorname{mod}(2^{10}, 11) &= 1 \\
\operatorname{mod}(2^{789}, 11) &= \operatorname{mod}(\operatorname{mod}(2^{10}, 11)^{78} \cdot \operatorname{mod}(2^9, 11), 11) \\
&= 6;
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{mod}(-23^1, 11) &= 10 \\
\operatorname{mod}(-23^2, 11) &= 1 \\
\operatorname{mod}(-23^{23}, 11) &= \operatorname{mod}(\operatorname{mod}(-23^2, 11)^{11} \cdot \operatorname{mod}(-23, 11), 11) \\
&= 10;
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{mod}(5^{31} \cdot 2^{789} - 23^{23}, 11) &= \operatorname{mod}(5 \cdot 6 + 10, 11) \\
&= \operatorname{mod}(40, 11) \\
&= 7
\end{aligned}
$$

(c) Bestimmen Sie $\operatorname{mod}(7^{31} \cdot 2^{789}, 10)$.
Bemerkung: Rechenweg ist gleich wie in Punkt (a).

$$
\begin{aligned}
\operatorname{mod}(7^{31}, 10) &= \operatorname{mod}(7^{16} \cdot 7^8 \cdot 7^4 \cdot 7^2 \cdot 7^1, 10) \\
&= \operatorname{mod}(1 \cdot 1 \cdot 1 \cdot 9 \cdot 7, 10) \\
&= \operatorname{mod}(63, 10) \\
&= 3
\end{aligned}
$$

$$
\operatorname{mod}(2^{789}, 10) = \operatorname{mod}(2^{512} \cdot 2^{256} \cdot 2^{16} \cdot 2^4 \cdot 2^1, 10)
$$

$$\begin{aligned}
&= \mathrm{mod}(6 \cdot 6 \cdot 6 \cdot 6 \cdot 2, 10) \\
&= \mathrm{mod}(12, 10) \\
&= 2
\end{aligned}$$

$$\begin{aligned}
\mathrm{mod}(7^{31} \cdot 2^{789}, 10) &= \mathrm{mod}(3 \cdot 2, 10) \\
&= \mathrm{mod}(6, 10) \\
&= 6
\end{aligned}$$

(d) Bestimmen Sie kgV(178, 144).

$$\begin{aligned}
178 &= 2 \cdot 89 \\
144 &= 2^4 \cdot 3^2 \\
\mathrm{kgV}(178, 144) &= 2^4 \cdot 3^2 \cdot 89 = 12816 && \text{(nach Lemma 1.5 (BM))}
\end{aligned}$$

(e) Bestimmen Sie ggT(12877480, 24145275).

$$\begin{aligned}
\mathrm{ggT}(12877480, 24145275) &= \mathrm{ggT}(24145275 - 12877480, 12877480) \\
&= \mathrm{ggT}(12877480 - 11267795, 11267795) \\
&= \mathrm{ggT}(11267795 - 1609685, 1609685) \\
&= 1609685 && \text{(nach Lemma 1.8 (BM))}
\end{aligned}$$

(f) Wie sieht der $\frac{12877480}{24145275}$ zu äquivalente teilerfremde Bruch aus?

$$\frac{12877480}{24145275} = \frac{2^3 \cdot 5 \cdot 7 \cdot 11 \cdot 37 \cdot 113}{3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 37 \cdot 113} = \frac{2^3}{3 \cdot 5}$$

(g) Wie viele Funktionen $f : \{0, 1, 2, 3\}^n \to \{0, 1, 2\}$ gibt es, die genau einmal den Funktionswert 0 annehmen?

(a) $\|\{0, 1, 2, 3\}^n\| = 4^n =_{def} m$

(b) $\|\{0, 1, 2\}\| = 3 =_{def} n$

Um 0 zu stellen haben wir m Möglichkeiten. Andere Zahlen, nämlich $n-1$, können wir an $m-1$ Stellen zu stellen. Dann mit so viel Kombinationen: $(n-1)^{m-1}$ bekommen wir:

$$m \cdot (n-1)^{m-1} = 4^n \cdot (3-1)^{4^n-1} = 4^n \cdot 2^{4^n-1} = 2^{4^n+2 \cdot n-1}$$

(h) Wie viele Funktionen $f : \{0, 1, 2, 3\}^n \to \{0, 1, 2\}$ gibt es, die genau zweimal den Funktionswert 0 annehmen?
Bemerkung: Definitionen (a) und (b) aus der Aufgabe (g) benutzt werden.
Um erste 0 zu Stellen haben wir m Möglichkeiten. Für die Zweiter haben wir $m-1$. Also für zwei 0: $m \cdot (m-1)$. Andere Zahlen, also $n-1$, können wir an $m-2$ Stellen zu stellen. Also mit so viel Kombinationen: $(n-1)^{m-2}$ Dann bekommen wir:

$$m \cdot (m-1) \cdot (n-1)^{m-2} = 4^n \cdot (4^n - 1) \cdot 2^{4^n-1}$$

(i) Wie viele Funktionen $f : \{0, 1, 2, 3\}^n \to \{0, 1, 2\}$ gibt es, die genau so oft die Funktionswerte 0 und 1 annehmen?
Bemerkung: Definitionen (a) und (b) aus der Aufgabe (g) benutzt werden.
Schreiben wir die Fälle, wenn 0 und 1 beide gar nicht zu einem Ergebnis kommen, wenn beide einmal, zweimal, usw.

$$\frac{m}{2} \begin{cases}
0: & 1 \\
1: & m \cdot (m-1) \\
2: & m \cdot (m-1) \cdot (m-2) \cdot (m-3) \\
\vdots & \\
m/2: & m \cdot (m-1) \cdot (m-2) \cdot (m-3) \cdot \ldots \cdot (m-(m-1))
\end{cases}$$

Dann wenn wir alle diese Fälle summieren - bekommen wir die Anzahl der Funktionen, die 0 und 1 genau so oft annehmen:

$$1+m+(m-1)+m\cdot(m-1)\cdot(m-2)\cdot(m-3)+\ldots+m\cdot(m-1)\cdot(m-2)\cdot(m-3)\cdot\ldots\cdot(m-(m-1))$$

(j) Sei $\|A\| =_{def} n$. Nach Lemma 4. $\|\{f|f:\{0,1\}\rightarrow A\}\| = n^2$. Nach Korollar 5. $\mathcal{P}(A) = 2^n$. Also haben wir: $\varphi : 2^n \rightarrow n^2$. Dann wieder nach Lemma 4. bekommen wir:

$$n^{2^{2^n}} = n^{2^{n+1}}$$

Transfer:

(a) 8 Symbole:

Schritt 1: Wir wählen beliebig zwei Sätze. Um Länge 8 zu bekommen mußen wir insgesamt 4 Wörtern haben, weil andere 4 Symbolen zusätzliche Zeichen sind.

Schritt 2: Da es in Alphabet 26 Buchstaben gibt, können wir von 4 kleine Buchstaben so viel Kombinationen machen:

$$26^4 = 456976$$

Schritt 3: Wenn eine halbe der Buchstaben gröss sein kann, dann verdoppelt unsere Zahl der Kombinationen:

$$(26)^4 \cdot 2 = 456976 \cdot 2 = 913952$$

Schritt 4: In Reihe von 4 Buchstaben können wir Ziffern in 7 Varianten stellen:

$$\begin{aligned}
&X \in 0,1,...,9\\
&\{a|bcd\} \rightarrow \{Xa|Xbcd\},\{aX|bcdX\}\\
&\{ab|cd\} \rightarrow \{Xab|Xcd\},\{aXb|cXd\},\{abX|cdX\}\\
&\{abc|d\} \rightarrow \{Xabc|Xd\},\{abcX|dX\}
\end{aligned}$$

Erste und zweite Zahlen kann 10 Ziffer sein. Also haben wir so viele Varianten für 2 Verschiedene Ziffern und 7 Satz Kombinazionen:

$$\begin{aligned}
&10 \cdot 10 \cdot 7 = 700\\
&913952 \cdot 700 = 639766400
\end{aligned}$$

Bemerkung: In dieser Schritt "eine Ziffer mit Bedeutung in die beiden Satzbereiche" gemäss Beispiel "LK1psDsIH2MG" war Interpretiert so, dass die Ziffern müssen "symmetrisch" in der Satz stehen (gleiche Stelle an beide Satzen haben).

Schritt 5: Nächstens haben wir 3 Möglichkeiten 6 Symbolen zu stellen:

$$\begin{aligned}
&3 \cdot 6 = 18\\
&639766400 \cdot 18 = 11515795200
\end{aligned}$$

Schritt 6: Dann haben wir 22 Symbole am Anfang oder am Ende:

$$\begin{aligned}
&22 \cdot 2 = 44\\
&11515795200 \cdot 44 = 506694988800
\end{aligned}$$

Da in diese Aufgabe ändert sich nur der Zahl der Symbole, kann man dazu ein Formel verwenden. Anzahl der Kombinationen in Schritt 4 kann man so berechnen:

$$k = \left(\frac{n}{2}\right)^2 + n - 1, \text{ wo n ist Anzahl der Symbole in Passwort minus 4.}$$

Dann gemäs der Informaton aus Schritten in (a) 1-6 bauen wir solche Funktion:

$$f(n) = 26^n \cdot 2 \cdot 10 \cdot 10 \cdot \left(\left(\frac{n}{2}\right)^2 + n - 1\right) \cdot 18 \cdot 44$$

(b) 10 Symbole: f(6) = 685051624857600

(c) 12 Symbole: f(8) = 760798761663283200

(d) 14 Symbole: f(10) = 760269510350821785600

(e) 16 Symbole: f(12) = 710449496554891463884800