DMat - Serie 10

Pascale Welsch
13-204-821

① Sei x eine gültige IBAN-Nummer, die aus 21 Zeichen besteht, wovon 2 Buchstaben sind. Es wird angenommen, dass die Buchstaben bereits durch je zwei Ziffern ersetzt wurden (gemäss Aufgabenstellung). Damit besteht die IBAN aus 23 Ziffern und kann als Zahl im Dezimalsystem interpretiert werden, gemäss:

$$a = a_{22}a_{21}\dots a_1 a_0 \quad , \text{ bzw. } \quad a = \sum_{i=0}^{22} a_i \cdot 10^i.$$

Im Falle eines Substitutionsfehlers unterscheidet sich eine fehlerhafte IBAN b von a in genau einer Stelle k. Es gilt $b_i = a_i$ für alle $i \neq k$ und $b_k = a_k + r$, wobei r der Fehler an Stelle k ist und $-a_k \leq r \leq 9 - a_k$ und $r \neq 0$.

Also gilt $\sum_{i=0}^{22} a_i \cdot 10^i \equiv 1 \pmod{97}$ und

$$b = \sum_{i=0}^{22} b_i \cdot 10^i = \left(\sum_{i=0}^{22} a_i \cdot 10^i\right) + \boxed{10^k \cdot r} \rightarrow \text{Fehler}$$

Beweis durch Kontradiktion: Angenommen, ein Substitutionsfehler lässt sich nicht feststellen, dann gilt

$$b = \sum_{i=0}^{22} b_i \cdot 10^i \equiv 1 \pmod{97} \quad \text{und damit auch}$$

$$b = \left(\sum_{i=0}^{22} a_i \cdot 10^i\right) + 10^k \cdot r \equiv 1 \pmod{97} \qquad (*)$$

Die einzige Möglichkeit, wie $(*)$ erfüllt sein kann ist, wenn $10^k \cdot r \equiv 0 \pmod{97}$. Und dies ist für $k \in \{0, \dots, 22\}$ nur möglich, falls $r = 0$ und in diesem Fall gäbe es gar keinen Substitutionsfehler $\rightarrow$ Widerspruch! □

Im Falle eines Transpositionsfehlers sind zwei Ziffern an den Stellen k und $k+1$ vertauscht, es gilt also $b_k = a_{k+1}$ und $b_{k+1} = a_k$ und für alle $i \neq k$, $i \neq k+1$ gilt $b_i = a_i$.

$r_k = b_k - a_k$ und $r_{k+1} = b_{k+1} - a_{k+1}$ sind die Fehler an den Stellen k und $k+1$. Zudem gilt, dass $r_k = -r_{k+1}$. Eine IBAN mit Transpositionsfehler lässt sich also folgendermassen ausdrücken:

$$
\begin{aligned}
b = \sum_{i=0}^{22} 10^i \cdot b_i &= \left(\sum_{i=0}^{22} 10^i \cdot a_i\right) + 10^k \cdot r_k + 10^{k+1} \cdot r_{k+1} \\
&= \left(\sum_{i=0}^{22} 10^i \cdot a_i\right) + 10^k \cdot r_k + 10^{k+1} \cdot (-r_k) \\
&= \left(\sum_{i=0}^{22} 10^i \cdot a_i\right) + \boxed{r_k\left(10^k - 10^{k+1}\right).} \longrightarrow \text{Fehler}
\end{aligned}
$$

Beweis durch Kontradiktion: Angenommen, ein Transpositionsfehler lässt sich nicht erkennen. Dann gilt

$b = \left(\sum_{i=0}^{22} 10^i \cdot a_i\right) + r_k\left(10^k - 10^{k+1}\right) \equiv 1 \pmod{97}$. Dies kann nur erfüllt sein, wenn $r_k \cdot (10^k - 10^{k+1}) \equiv 0 \pmod{97}$. Da $97 \nmid 10^k - 10^{k+1}$ für $0 \leq k < 22$ ist dies nur erfüllt, falls $r_k = 0$, was widerum heisst, dass kein Transpositionsfehler vorliegt. $\Rightarrow$ Widerspruch! $\square$

Bonusfrage: Bei mod 97 ist die Wahrscheinlichkeit am grössten einen Fehler zu erkennen, weil es die grösste zweistellige Primzahl ist (z.B. ist eine Zahl durch 99 teilbar, wenn sie durch 9 und durch 11 teilbar ist). Die Wahrscheinlichkeit, dass ein Fehler in der IBAN zu einer Zahl führt, für die ebenfalls gilt dass IBAN $\equiv 1$ modulo (97)

② Der egcd-Algorithmus kann nur dann zum Finden
a) eines Inversen modulo m verwendet werden wenn gilt, dass
$gcd(a,m) = 1$, weil dann

$$s \cdot a + t \cdot m = 1 \quad \text{und folglich}$$
$$s \cdot a + t \cdot m \equiv 1 \pmod m \quad \text{gilt.}$$

Da $t \cdot m$ ein Vielfaches von m ist, gilt $t \cdot m \equiv 0 \pmod m$ und folglich $s \cdot a \equiv 1 \pmod m$. s ist also gerade ein Inverses modulo m von a, weil für ein Inverses $\bar{a}$ modulo m von a gelten muss, dass

$$a \cdot \bar{a} \equiv 1 \ (\text{modulo } m).$$

Wenn $gcd(a,m) \neq 1$, dann auch

$$s \cdot a + t \cdot m \neq 1 \quad \text{und}$$
$$s \cdot a + t \cdot m \not\equiv 1 \pmod m \quad (\text{weil } gcd(a,m) \leq m).$$

Für $t \cdot m$ gilt immer noch $t \cdot m \equiv 0 \pmod m$ und damit $s \cdot a \not\equiv 1 \pmod m$.

Deshalb ist es zwar möglich, dass der egcd-Algorithmus terminiert und ein s liefert, welches aber dann kein Inverses modulo m von a ist. z.B. für
$a = 33$, $b = m = 6$

q	a	b	s	s'	t	t'
	33	6	1	0	0	1
5	6	3	0	1	1	-5
2	3	0	1	-2	-5	

$\rightarrow gcd = 3$
$s = 1$

$$33 \cdot 1 \equiv 3 \pmod 6 \not\equiv 1 \pmod 6 \ !$$

b) Da m zusammengesetzt ist gemäss $m = p \cdot q$, p prim und q prim, kann es sein, dass $\gcd(a,m) \neq 1$, sondern $\gcd(a,m) = p$ oder $\gcd(a,m) = q$. In diesen Fällen wäre das s, das der egcd-Algorithmus liefert, kein Inverses modulo m von a. Das heisst auch, dass wenn $s \cdot a \not\equiv 1 \pmod{m}$, dann muss der $\gcd(a,m)$ entweder p oder q sein. Man könnte diesen Algorithmus somit verwenden um mithilfe zufälliger a die Primfaktoren von m zu „erraten". Dies ist aber immer noch sehr ineffizient. **

3 a) Der kleine Fermatsche Satz besagt, dass die Sequenz $a^1, a^2, \dots \pmod{p}$ zyklisch ist. Wenn man eine Zahl n mit a^{p-1} modulo p multipliziert, erhält man dasselbe Ergebnis, wie wenn man n mit 1 modulo p multipliziert.

$$
\begin{aligned}
a^0 &\equiv 1 \pmod{p} \quad \big\downarrow \cdot a \\
a^0 \cdot a^1 &\equiv a^1 \pmod{p} \\
&\vdots \\
a^{p-1} &\equiv 1 \pmod{p} \quad \big\downarrow \cdot a \\
a^p &\equiv a \pmod{p} \quad \big\downarrow \cdot a \\
&\vdots \\
a^x &\equiv a^{x \pmod{p-1}} \pmod{p}
\end{aligned}
$$

Da $x \equiv y \pmod{p-1}$ wird die letzte Kongruenz zu $a^x \equiv a^y \pmod{p}$ $\square$

b) Es ist möglich, dass für x,y wobei
$a^x \equiv a^y \pmod p$ gilt, dass
$x \not\equiv y \pmod{p-1}$

z.B. für $a=2$, $p=7$

$2^0 \bmod 7 = 1$
$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$
$2^4 \bmod 7 = 2$
$2^5 \bmod 7 = 4$
$2^6 \bmod 7 = 1$
$2^7 \bmod 7 = 2$

Hier gilt $2^4 \equiv 2^1 \pmod 7$,
aber $4 \not\equiv 1 \pmod 6$!

c) $100 \bmod 18 = 10$
$\Rightarrow 2^{100} \equiv 2^{10} \pmod{19}$

$2^1 \bmod 19 = 2$
$2^2 \bmod 19 = 4$
$2^3 \bmod 19 = 8$
$2^4 \bmod 19 = 16$
$2^5 \bmod 19 = 13$
$2^6 \bmod 19 = 7$
$2^7 \bmod 19 = 14$
$2^8 \bmod 19 = 9$
$2^9 \bmod 19 = 18$
$2^{10} \bmod 19 = \underline{\underline{17}}$ $\rightarrow$ $2^{100} \bmod 19 = \underline{\underline{17}}$

$123 \bmod 10 = 3$ $\Rightarrow$ $3^{123} \equiv 3^3 \bmod 11$

$3^1 \bmod 11 = 3$
$3^2 \bmod 11 = 9$
$3^3 \bmod 11 = \underline{\underline{5}}$ $\rightarrow$ $3^{123} \bmod 11 = \underline{\underline{5}}$

$310 \bmod 102 = 4$ $\Rightarrow$ $4^{310} \equiv 4^4 \bmod 103$

$4^1 = 4 \bmod 103$
$4^2 = 16 \bmod 103$
$4^3 = 64 \bmod 103$
$4^4 = 50 \bmod 103$ $\rightarrow$ $4^{310} \bmod 103 = \underline{\underline{50}}$

(4) Damit $\bar{a}$ invers modulo p zu a ist, muss gelten:

$a \cdot \bar{a} \equiv 1 \pmod{p}$

Der kleine Fermatsche Satz besagt, dass

$a^{p-1} \equiv 1 \pmod{p}$

Da $a^{p-1} = a \cdot a^{p-2}$ gilt

$a \cdot a^{p-2} \equiv 1 \pmod{p}$ und somit

ist a^{p-2} ein Inverses modulo p von a.

** Folglich muss auch für jedes $a < m$ und $a \neq p$, $a \neq q$ ein Inverses modulo m existieren.