TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik • Institut für Algebra • Prof. Bodirsky, Dr. Noack

Einführung in die Mathematik für Informatiker: Diskrete Strukturen INF 110
Wintersemester 2019/20

8. Lösungsblatt

für die Woche 09.12. - 15.12.2019

Gruppen, Untergruppen, Euler-Fermat, Verschlüsselung

Ü45 Das RSA-Verfahren soll mit kleinen Zahlen getestet werden. Man nehme p=7 und q=11.

(a) Der öffentliche Schlüssel sei e=23. Berechnen Sie den privaten Schlüssel d.

(b) Verschlüsseln Sie mit dem öffentlichen Schlüssel aus (a) die Zahl m=12.
(Überprüfen Sie das Ergebnis durch Entschlüsselung mit dem privaten Schlüssel.)

Lösung:

(a) $n = p \cdot q = 77 \Rightarrow \varphi(n) = 6 \cdot 10 = 60$.
Mit Euklidischem Algorithmus multiplikativ Inverses zu $e = 23$:
$1 = 5 \cdot 60 - 13 \cdot 23 \Rightarrow d = 60 - 13 = 47$.

(b) Verschlüsselung von $m = 12$: $m^e = 12^{23} \pmod{77}$.
$23 = 2^4 + 2^2 + 2 + 1 \Rightarrow 12^{23} = ((12^{2\cdot 2} \cdot 12)^2 \cdot 12)^2 \cdot 12 \equiv ... \pmod{77}$.

(c) Entschlüsselung: $...^d = ...^{47} \equiv m \pmod{77}$:
$47 = 2^5 + 2^3 + 2^2 + 2 + 1 \Rightarrow ....^{47} = \Big(((.....^{2\cdot 2} \cdot ....)^2 \cdot .....)^2 \cdot .....\Big)^2 \cdot .... \equiv 12 \pmod{77}$.

H47 Es seien $(G; \circ)$ eine Gruppe und $a, b \in G$ beliebige Elemente. Beweisen Sie, dass für die Linksnebenklassen einer beliebigen Untergruppe U von G folgende Aussagen äquivalent sind (d.h. für jedes Paar aus den drei Aussagen gilt die eine genau dann, wenn die andere gilt):

(a) $a \circ U = b \circ U$,

(b) $b \in a \circ U$,

(c) $a^{-1} \circ b \in U$.

Hinweis: Beweisen Sie dazu folgende Kette von Implikationen: (a) ⇒ (b) ⇒ (c) ⇒ (a).
Lösung:

(a)⇒(b)

Da $e \in U$ ist, folgt wegen (a), dass $b \circ e \in b \circ U = a \circ U \Rightarrow b \in a \circ U$.

(b)⇒(c)

Wegen (b) existiert ein $u \in U$ mit $b = a \circ u$. Daraus folgt sofort $a^{-1} \circ b = u \in U$.

(c)⇒(a)

Da $a^{-1} \circ b \in U$ ist, gibt es ein $u \in U$ mit $a^{-1} \circ b = u$ und folglich $b = a \circ u$.

Zeigen nun $a \circ U \subseteq b \circ U$ und $b \circ U \subseteq a \circ U$ (und damit '=').

Es sei $x \in a \circ U$ beliebig $\Rightarrow$ $x = a \circ \tilde{u}$ für ein $\tilde{u} \in U$ $\Rightarrow$ $x = \underbrace{a \circ u}_{=b} \circ \underbrace{u^{-1} \circ \tilde{u}}_{\in U} \in b \circ U$.

$\Rightarrow a \circ U \subseteq b \circ U$.

Es sei $y \in b \circ U$ beliebig $\Rightarrow$ $y = b \circ \overline{u}$ für ein $\overline{u} \in U$ $\Rightarrow$ $y = a \circ \underbrace{u \circ \overline{u}}_{\in U} \in a \circ U$.

$\Rightarrow b \circ U \subseteq a \circ U$.

H48 Verwenden Sie bei den folgenden Aufgaben den Satz von Euler-Fermat:

(a) Berechnen Sie die letzten zwei Ziffern der Zahl 211^{1043}.

(b) Zeigen Sie, dass für zwei beliebige Primzahlen p und q mit $p \neq q$ und jede Zahl $a \in \mathbb{Z}$, die nicht durch p oder q teilbar ist, gilt:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}.$$

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

Lösung:

(a) Es ist $211^{1043} \pmod{100}$ zu berechnen. Es ist $267^{1043} \equiv 11^{1043} \pmod{100}$ und $\mathrm{ggT}(11, 100) = 1$. Folglich gilt nach dem Satz von Euler-Fermat und mit $\phi(100) = \phi(2^2) \cdot \phi(5^2) = 2 \cdot 4 \cdot 5 = 40$:

$$11^{1043} \equiv 11^{1043 \,(\mathrm{mod}\ \phi(100))} \equiv 11^{1043 \,(\mathrm{mod}\ 40)} \equiv 11^3 \equiv 21 \cdot 11 = 31 \,(\mathrm{mod}\ 100).$$

(b) 1. Weg: $n := p \cdot q$ $\Rightarrow$ $\varphi(n) = n(1 - \frac{1}{p})(1 - \frac{1}{q}) = (p-1)(q-1)$. Folglich mit Euler-Fermat:

$a^{\varphi(n)} = a^{(p-1)(q-1)} \equiv 1$ (mod pq).

2. Weg: kleiner Fermat: $a^{p-1} \equiv 1$ (mod p) und $a^{q-1} \equiv 1$ (mod q)

$\Rightarrow$ $a^{(p-1)(q-1)} \equiv 1$ (mod p) und $a^{(p-1)(q-1)} \equiv 1$ (mod q).

Folglich existieren $k, l \in \mathbb{N}:$ $a^{(p-1)(q-1)} - 1 = kp = lq$. Da $p \neq q$ Primzahlen sind,

gilt $q|k$ und $p|l$. Also ex. $m \in \mathbb{N}$ mit $a^{(p-1)(q-1)} - 1 = mpq$ $\Rightarrow$ Behauptung gilt.

(c) $\frac{1}{5}m^5 + \frac{1}{3}m^3 + \frac{7}{15}m$ ist eine natürliche Zahl.

$\frac{1}{5}m^5 + \frac{1}{3}m^3 + \frac{7}{15}m = \frac{3m^5 + 5m^3 + 7m}{15}$.

Der Zähler ist durch $3 \cdot 5 = 15$ teilbar, denn mit dem kleinen Satz von Fermat folgt:
$3m^5 + 5m^3 + 7m \equiv 2m^3 + m \equiv m(2m^2 + 1) \equiv m(2 + 1) \equiv 0 \pmod{3}$ und
$3m^5 + 5m^3 + 7m \equiv 3m^5 + 2m \equiv m(3m^4 + 2) \equiv m(3 + 2) \equiv 0 \pmod{5}$.