KRY: Wahlfach Kryptologie
Serie 5: Primzahltests, diskrete Logarithmen

Aufgabe 1 (T)

(a) Für diese Teilaufgabe setzen wir $n = 21$.

(i) Bestimmen Sie die Menge der Fermat-Lügner von n.

(ii) Wie viele zufällige $a \in \mathbb{N}$ mit $1 \leq a \leq 20$ muss man mindestens wählen (Ziehen mit Zurücklegen), damit der Fermat-Test (hier ohne Probedivisionen mit kleinen Primteilern) die Zahl n mit mindestens 99% Wahrscheinlichkeit als zusammengesetzt erkennt?

(b) Bezüglich welcher Elemente der Menge $A = \{18, 21, 23, 38\}$ ist 221 eine Pseudoprimzahl?

(c) Begründen Sie mit Hilfe des Fermat-Tests, dass $n = 8051$ zusammengesetzt ist.

Aufgabe 2 (T)

Wir setzen $n := 3'828'001$.

(a) Begründen Sie, dass für jedes $a \in \mathbb{Z}_n^*$ gilt: $a^{n-1} = 1 \pmod{n}$.
Tipp: Zeigen Sie, dass n eine Carmichael Zahl ist.

(b) Benutzen Sie den Miller Rabin Test zusammen mit einem geeigneten a, um zu belegen, dass n zusammengesetzt ist.

Aufgabe 3 (T)

Wir setzen $p = 17$. Erstellen Sie eine Tabelle, die zu jedem $a \in \{1, \ldots, p-1\}$ die diskreten Logarithmen $\log_g(a)$ in $\mathbb{Z}_p^*$ für die Basen $g = 7$ und $g = 13$ angibt, falls sie existieren.

1. a.i) $n = 21$

$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$FL(n) = \{a \in \mathbb{Z}_n^* : a^{n-1} = 1 \pmod n\}$

a	1	2	4	5	8	10	11	13	16	17	19	20
$a^{20} \bmod 21$	1	4	16	4	1	16	16	1	4	16	4	1

$FL(21) = \{1, 8, 13, 20\}$ $\quad |FL(21)| = 4$

ii) Wahrscheinlichkeit für $FL(21) = \frac{4}{20} = \underline{0{,}2}$

$1 - (0{,}2)^x = 0{,}99$ $\qquad$ solve$\left(1-(0.2)^x=0.99,x\right)$ ▸ $x=2.8613531$

TI Nspire

$\hookrightarrow x = 2{,}861$

$\hookrightarrow$ 3 Ziehungen

b) $A = \{18, 21, 23, 38\}$

$n = 221 \qquad a^{n-1} \bmod n = 1$

$$\left.\begin{array}{l} 1.\ 18^{220} \bmod 221 = 1 \\ 2.\ 21^{220} \bmod 221 = 1 \\ 3.\ 23^{220} \bmod 221 = 81 \\ 4.\ 38^{220} \bmod 221 = 1 \end{array}\right\} = \{18, 21, 38\}$$

c) $n = 8051 \qquad a = 2$

$2^{8050} \bmod 8051 = 2274 \neq 1$

$\hookrightarrow$ zusammengesetzt

Fermat Test

for $i = 1$ **to** t **do**

Erzeuge eine Zufallszahl a mit $1 \leq a \leq n-1$

Berechne $r := a^{n-1} \pmod n$

if $((r \neq 1)$ **or** $(\mathrm{ggT}(a, n) \neq 1))$ **then return** "nicht prim"

end

return "prim"

2. $n = 3'828'001$

a) $3'828'001 = 101 \cdot 151 \cdot 251$ — pari factor(n)

$\to n =$ ist quadratfrei

Satz (ohne Herleitung)

Für jede zusammengesetzte Zahl $n \geq 3$ gilt: n ist Carmichael Zahl $\Leftrightarrow$
(1) n ist quadratfrei, und
(2) für jeden Primteiler p von n gilt $(p-1) | (n-1)$

$100 \mid 3'828'000 \to \checkmark$
$150 \mid$ " $\to \checkmark$
$250 \mid$ " $\to \checkmark$

Folgerung

Für jede Carmichael-Zahl n gilt:
(1) n besitzt mindestens 3 Primfaktoren.
(2) n ist ungerade.

b) $n-1 = 2^r \cdot u$

$r = 5$
$u = 119'625$

solve$(n-1=2^5 \cdot x, x)$ ▸ $x=119625$

$a^u \bmod n = 1$

$2^{119625} \bmod 3828001 = 2'879'722$
$\neq 1 \neq -1$

%1 = Mod(2879722, 3828001)

$2^{2 \cdot 119'625} \bmod 3'828'001 = 1'174'932$
$\neq -1$

$2^{4 \cdot 119'625} \bmod n = 1 \neq -1$

3. $p = 17$ $\quad a = \{1, \ldots, p-1\}$ $\quad g_1 = 7$ $\quad g_2 = 13$

Hilfstabelle

pari

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$7^x \bmod p$	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
$13^x \bmod p$	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\log_7(a)$	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8
$\log_{13}(a)$	4 8 12 16	–	–	3 7 11 15	–	–	–	–	–	–	–	–	1 5 9 13	–	–	2 6 10 14