KRY: Wahlfach Kryptologie
Serie 5: Primzahltests, diskrete Logarithmen

Aufgabe 1 (T)

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

n= 21 -> factor(21) = 3,7

a = {1,2,4,5,8,10,11,13,16,17,19,20}

a^20 mod 21 = 1, 4, 16, 4, 1, 16, 16, 1, 4, 16, 4, 1

(i) Bestimmen Sie die Menge der Fermat-Lügner von n. Fermet Lügner = {1, 8, 13, 20}

(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? Anzahl Lügner = 4 / 20 -> Wahrscheinlichkeit = 4/20 = 1/5 = 0.2

1-(0.2)^k >= 0.99 | k >= ln(0.01)/ln(0.2)= 2.86 -> 3

(b) Bezüglich welcher Elemente der Menge $A = \{18, 21, 23, 38\}$ ist 221 eine Pseudoprimzahl? a ^ (n−1) = 1 (mod n) und ggT(a, n) = 1.

ggt(18,221), ggt(18,221), ggt(18,221), ggt(18,221) = 1

18 ^ 220 mod 221 = 1
21 ^ 220 mod 221 = 1
23 ^ 220 mod 221 = 81
38 ^ 220 mod 221 = 1 Pseudobasis zu {18,21,38}

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

Bedingung: 1 < a < n und ggT(a, n) > 1 a = 3569 und ggt(1950, 8051) = 1

a beliebig = 1955 -> 1955 ^ 8050 mod 8051 => 5869 != 1 n ist zusammgengesetzt!

Aufgabe 2 (T)

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

Aufgabe 3 (T)

Bestimmen Sie den prozentualen Anteil der natürlichen Zahlen, die durch mindestens eine der ersten Primzahlen bis und mit 13 teilbar sind.

Aufgabe 4 (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.

Aufgabe 2)

a mit ggt(a,n) = 1 dann: a ^ (n-1) = 1 mod n

n ist Carmichal Zahl wenn
1) n ist quadratfrei
2) für jeden Primteiler p von n gilt (p-1) | (n-1)

1) 3828001 mod 2 = 1 -> ungerade!
2) factor(3828001) = 101, 151, 251
101 - 1 | 3828001-1, 151 - 1 | 3828001-1, 251 - 1 | 3828001-1
Alle Primfaktoren können n teilen!
Beide Bedingungen erfüllt!

-> n ist eine Carmichalzahl: a^(2828001-1) = 1 mod 3828001

Aufgabe 3)

Primzahlen (p) = {2,3,5,7,11,13}, Suche nach Zahlen, wo nicht durch p teilbar sind -> 1 - 1/p!
1-1/2= 0.5, 1-1/3= 0.667, 1-1/5= 0.8, 1-1/7= 0.8571, 1-1/11= 0.90909, 1-1/13= 0.9230769 = 192/1001

1- 192/1001 = 809/1001 = 0.80819 -> Lösung = 80.82%

Aufgabe 4)

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
7^x mod 17	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
log7(x)	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8
13^x mod 17	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
log13(x)	4			3									1			2
	8			7									5			6
	12			11									9			10
	16			15									13			14