Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2015/16
21. Okt. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 1

Aufgabe 1

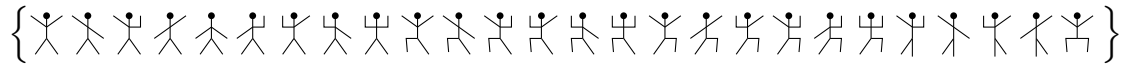
Bekanntlich gibt es $26! = 40\,32914\,61126\,60563\,55840\,00000$ Permutationen der Menge $\mathbb{Z}_{26} \cong \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$. Man zeige, dass davon $25\,49288\,23778\,13549\,97627\,12175$ Permutationen, also etwa 63%, einen Fixpunkt besitzen. (Ein Fixpunkt einer Permutation $\pi : \mathfrak{A} \to \mathfrak{A}$ ist ein Element $x \in \mathfrak{A}$ mit $\pi(x) = x$.)

Anleitung. Man beweise dazu folgende allgemeine Formel: Für die Anzahl $N_f(n)$ aller Permutationen einer n-elementigen Menge, die einen Fixpunkt besitzen, gilt

$$N_f(n) = n!\Big(\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}\Big).$$

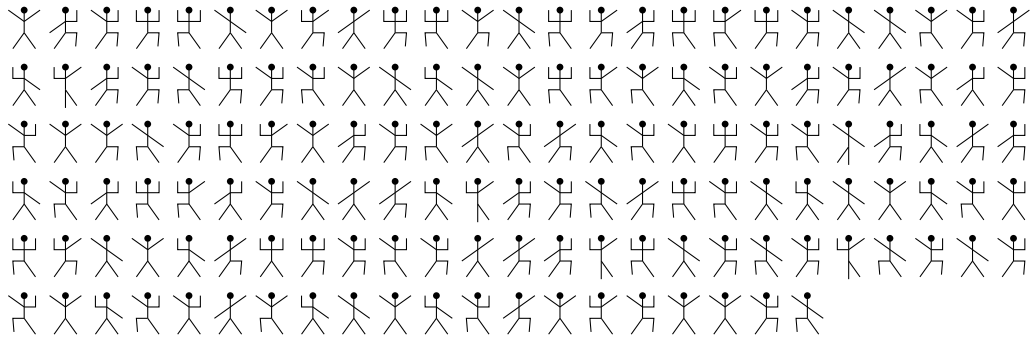
Aufgabe 2

Das folgende Geheimtext-Alphabet

$\mathfrak{B} :=$ 

einer monoalphabetischen Substitution $\pi : \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}\} \to \mathfrak{B}$ stammt (in abgewandelter Form) aus einer Kurzgeschichte von Arthur Conan Doyle.

Man entschlüssele den folgenden Geheimtext, der aus einem englischen Klartext mittels einer solchen Substitution entstand.



Hinweise. a) Die häufigsten Buchstaben im Englischen sind

E	T	R	N	I	O	A	S
12.75	9.25	8.5	7.75	7.75	7.5	7.25	6

Die Häufigkeiten sind in Prozenten angegeben. Bei kürzeren Texten ergeben sich natürlich mehr oder weniger große Abweichungen.

b) Das häufigste Trigramm im Englischen ist `THE`.

c) Der Klartext enthält das Wort `HOLMES`.

Aufgabe 3

Es sei $\mathrm{GL}(2, \mathbb{Z}_{26})$ die Menge aller invertierbaren 2×2-Matrizen mit Koeffizienten aus $\mathbb{Z}_{26}$ und $\mathrm{Aff}(2, \mathbb{Z}_{26})$ die Menge aller Abbildungen

$$\psi : Z_{26}^2 \to \mathbb{Z}_{26}^2, \quad x \mapsto \psi(x) := Ax + t, \quad A \in \mathrm{GL}(2, \mathbb{Z}_{26}),\ t \in \mathbb{Z}_{26}^2.$$

a) Man zeige, dass $\mathrm{Aff}(2, \mathbb{Z}_{26})$ bzgl. der Komposition von Abbildungen eine Gruppe bildet. Aus wievielen Elementen besteht diese Gruppe?

b) Vermöge der Identifikation $\{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \cong \mathbb{Z}_{26}$ kann man die Elemente aus $\mathrm{Aff}(2, \mathbb{Z}_{26})$ als Bigramm-Substitutionen auffassen. Man bestimme, falls möglich, Transformationen aus $\mathrm{Aff}(2, \mathbb{Z}_{26})$, die `ALBERT` in `JOSEPH` bzw. in `JOHANN` überführen.

Aufgabe 4

a) Die Folge $(f_k)_{k \geqslant 0}$ der Fibonacci-Zahlen ist rekursiv definiert durch

$$f_0 := 0, \quad f_1 := 1, \quad f_{k+1} := f_k + f_{k-1} \quad \text{für } k \geqslant 1.$$

Man beweise

$$f_k = \frac{1}{\sqrt{5}} \left(\gamma^k - \left(\frac{-1}{\gamma} \right)^k \right) \qquad \text{mit} \quad \gamma := \tfrac{1}{2}(1 + \sqrt{5}).$$

b) Aus a) leite man folgende Aussage zur Komplexität des Euklidischen Algorithmus ab: Die Anzahl r der Schritte, die zur Berechnung des größten gemeinsamen Teilers zweier natürlicher Zahlen $x \geqslant y > 0$ nötig sind, genügt der Abschätzung $r = O(\log x)$.
