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

WS 2015/16
13. Jan. 2016

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 10

Aufgabe 37

Sei M eine endliche Menge und $f : M \to M$ eine Abbildung. Durch f kann man auf M die Struktur eines gerichteten Graphen wie folgt einführen. Die Punkte des Graphen sind die Elemente von M. Genau dann werden Punkte $a, b \in M$ durch eine von a nach b gerichtete Kante verbunden, wenn $f(a) = b$. Eine Folge von Punkten $(a_1, a_2, \ldots, a_k)$ heißt Zyklus, wenn es gerichtete Kanten von a_i nach a_{i+1}, $(1 \leqslant i < k)$, sowie von a_k nach a_1 gibt. Im Spezialfall $k = 1$ besteht der Zyklus aus einem Fixpunkt der Abbildung f. Ein Punkt $a \in M$ heißt Quelle, wenn von a eine Kante ausgeht, aber keine Kante in a mündet.

a) Sei p eine ungerade Primzahl, $M := \mathbb{Z}/p$ und $f : M \to M$ die durch $f(x) := x^2 + 2$ definierte Abbildung. (Diese Abbildung kommt beim Pollardschen Rho-Faktorisierungs-Algorithmus vor.) Man zeige:

i) Die Anzahl der Quellen ist gleich $(p-1)/2$.

ii) Für $p \neq 7$ gibt es Fixpunkte (und zwar zwei) genau dann, wenn $\left(\dfrac{-7}{p}\right) = 1$.

iii) Für $p = 7$ gibt es genau einen Fixpunkt.

b) In den Spezialfällen $p = 41$ und $p = 43$ zeichne man den durch die in a) definierte Abbildung gegebenen gerichteten Graphen.

Aufgabe 38*

Für $n \geqslant 1$ ist die Abbildung

$$f : (Z/2^n)^* \longrightarrow (Z/2^n)^*, \quad x \mapsto x(2x+1) \bmod 2^n,$$

bijektiv, vgl. Aufgabe 24a).

Man beweise: Der durch diese Abbildung definierte gerichtete Graph besteht aus einem einzigen Zyklus der Länge 2^{n-1}.

Aufgabe 39

Der Fermatsche Algorithmus zur Faktorisierung einer zusammengesetzten ungeraden Zahl $N \geqslant 9$ arbeitet bekanntlich wie folgt: Mit $x_0 := \lceil \sqrt{N} \rceil$ berechne man für $x := x_0 + k$, $k = 0, 1, 2, 3, \ldots$, der Reihe nach die Differenzen $x^2 - N$, bis sich eine Quadratzahl ergibt:

$$x^2 - N = y^2.$$

Dann ist $N = (x-y)(x+y)$ eine nicht-triviale Faktorzerlegung von N.

---

b.w.

a) Man beweise, dass der Algorithmus stets nach einer endlichen (evtl. sehr großen) Anzahl von Schritten erfolgreich ist.

b) Sei $N = uv$ mit positiven ganzen Zahlen u, v, die der Abschätzung $|u - v| \leqslant \alpha \sqrt[4]{N}$ mit einer (nicht zu großen) reellen Konstanten α genügen. Man schätze (als Funktion von α) die Anzahl der Schritte ab, die der Fermatsche Algorithmus zur Faktorisierung von N braucht.

Aufgabe 40

Um ein RSA-System mit Modul $N = pq$, wobei $2^{2m-1} < N < 2^{2m}$, (z.B. $m = 512$) aufzustellen, wird empfohlen, die Primzahlen p, q so zu wählen, dass

$$|p - q| \geqslant 2^{m-7}.$$

a) Warum ist das Fermatsche Faktorisierungs-Verfahren zur Faktorisierung von N dann ungeeignet?

b) Im folgenden Beispiel eines RSA-Moduls N wurde diese Empfehlung nicht beachtet. In hexadezimaler Schreibweise ist

```
 N = B679 98BE 9984 1D72 8857 EC8F 820F BDCA F6D7 4714 AB90 B7F3 3CD8 031B
8EE3 32A7 9966 AF89 A727 4CB1 AD90 EF92 005D C74E 1AE5 DFD8 A0B4 8A1B 6D73
3CA9 4096 9DD9
```

Der Verschlüsselungs-Exponent ist $e = 2^{16} + 1$. Man enschlüssele den folgenden Geheimtext

```
 y = A67B 49EB 8F99 0EC8 F6FD 326F 48CA 8F54 3820 49E7 DBAE 485C D8C0 3445
FF3C 2169 DE76 53DC 7AD1 0C40 35F2 4CA5 474F B86E F1CF FECE A32D 9715 9BFE
408F F6A2 64B1
```

Dieser entstand aus einem Ascii-Klartext $(a_1, a_2, \ldots, a_n)$, $0 \leqslant a_i < 256$, der durch eine ganze Zahl

$$x = \sum_{i=1}^{n} a_i \cdot 256^{n-i}$$

dargestellt wurde.

---

* Die korrekte und selbständige Lösung der Aufgabe 38* wird mit einem Notenbonus von 0.3 belohnt. Lösungen können in der Vorlesung (am Mittwoch oder Freitag) abgegeben werden.