Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 10
13. Januar 2016

Übungen zur Algorithmischen Zahlentheorie

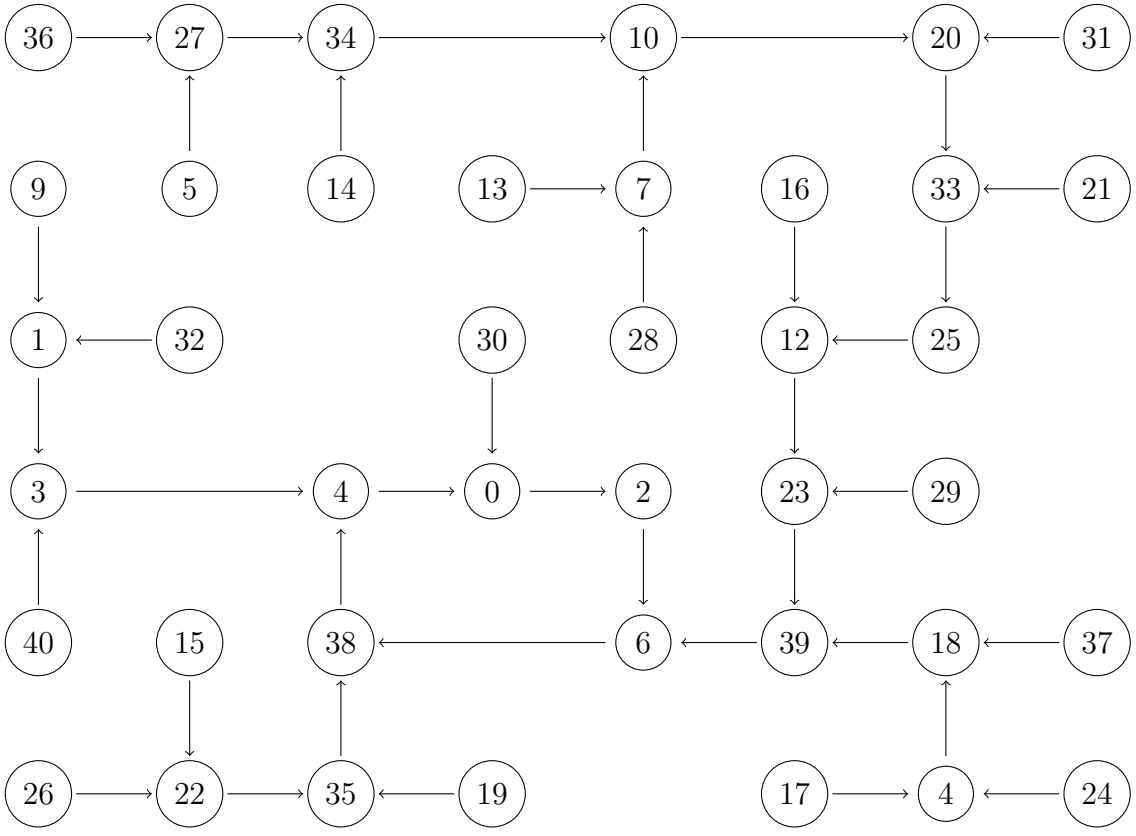
Aufgabe 37

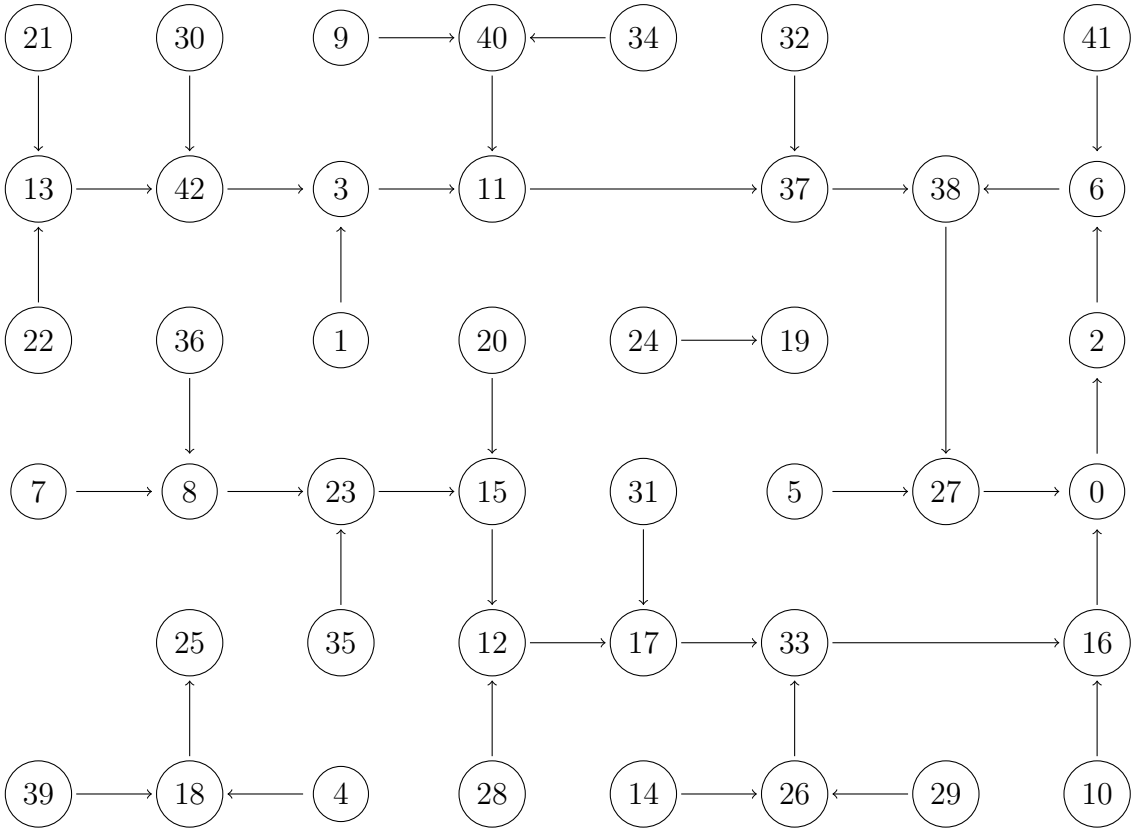
a) i) Wir müssen die Anzahl der Elemente des Bildes $f(\mathbb{Z}/p)$ berechnen. Die Aussage folgt aus:
Satz. Für eine zyklische Gruppe der Ordnung m hat der Endomorphismus $f_k : x \mapsto x^k$ ein Bild der Mächtigkeit $m/\gcd(k,m)$.
Beweis. Wir wieder den Beweis aus Prof. Forsters Buch zur Algorithmischen Zahlentheorie, 14.1. Sei $\langle g\rangle = G$ und $d = \gcd(k,m), dj = k$, so erzeugt g^d das Bild von f_k, denn aus $d = \nu k + \mu m$ folgt für alle $y = x^k = (g^i)^k = (g^i)^{jd} = (g^d)^{ij}$, dass $y \in \langle g^d\rangle$. Man beachte $g^d = g^{\nu k} = (g^\nu)^k$ liegt selbst im Bild. Wir haben gezeigt, dass das Bild gerade aus den Elementen $(g^d)^n$ mit $0 \leqslant n < \frac{m}{d}$ besteht. □
Damit wissen wir, dass $f_2((\mathbb{Z}/p)^*) = \frac{p-1}{2}$ und es somit $\frac{p-1}{2}$ Quellen von f_2 in $(\mathbb{Z}/p)^*$. Da $f_2(0) = 0$ ist 0 keine Quelle, also gibt es $\frac{p-1}{2}$ Quellen von f_2 in $\mathbb{Z}/p$ und damit auch $\frac{p-1}{2}$ Quellen von f in $\mathbb{Z}/p$.

ii) Nach Aufgabe 21 hat $ax^2 + bx + c = 0, p \nmid a$ genau $1 + \left(\frac{b^2-4ac}{p}\right)$ Lösungen. Für $x^2 - x + 2 = 0$ ergeben sich $1 + \left(\frac{-7}{p}\right)$ Lösungen.

iii) Siehe ii).

b) Wir zeichnen die beiden Falle 41 und 43 nacheinander:





Aufgabe 38*

Wir betrachten f_n je nach Kontext als eine der Abbildungen $f_n : \mathbb{Z}/2^n \to \mathbb{Z}/2^n,\ x \mapsto x(2x+1)$ oder $f : \mathbb{Z} \to \mathbb{Z},\ x \mapsto x(2x+1) \bmod 2^n$.
Die Behauptung für $n = 1$ ist trivial. Sei deshalb $n \geqslant 2$. Wir benötigen die folgende Aussage:

Behauptung 1. Für alle $n \geqslant 2$ und alle $a, b \in \mathbb{Z}$ gilt

$$f_{n+1}(x + a \cdot 2^{n-1} + b \cdot 2^n) = f_{n+1}(x) + a \cdot 2^{n-1} + b \cdot 2^n, \quad \forall x \in (\mathbb{Z}/2^{n+1})^*.$$

Beweis von Behauptung 1. Wir berechnen

$$\begin{aligned} f_{n+1}(x + a \cdot 2^{n-1} + b \cdot 2^n) &= (x + a \cdot 2^{n-1} + b \cdot 2^n)(2((x + a \cdot 2^{n-1} + b \cdot 2^n)) + 1) \\ &= 2x^2 + ax \cdot 2^n + bx \cdot 2^{n+1} + x + ax \cdot 2^n + a^2 \cdot 2^{2n-1} + ab \cdot 2^{2n} \\ &\quad + a \cdot 2^{n-1} + bx \cdot 2^{n+1} + ab \cdot 2^{2n} + b^2 \cdot 2^{2n+1} + b \cdot 2^n \\ &= f_{n+1}(x) + a \cdot 2^{n-1} + b \cdot 2^n. \end{aligned}$$

□

Behauptung 2. Für alle $n \geqslant 2$ gilt $f_{n+1}^{2^{n-1}}(x) = x + 2^n$ für alle $x \in (\mathbb{Z}/2^{n+1})^*$.[1]

Beweis von Behauptung 2. Wir zeigen die Aussage mit Induktion nach n. Den Induktionsanfang $n = 2$ liefert die Periode $1 \mapsto 3 \mapsto 5 \mapsto 7 (\mapsto 1)$.
Man beachte es gilt $f_n(x \bmod 2^n) = f_{n+1}(x) \bmod 2^n$ für alle $x \in (\mathbb{Z}/2^{n+1})^*$. Somit ist $f_{n+1}(x) = f_n(x) + b \cdot 2^n$ mit $b \in \{0, 1\}$ oder allgemeiner $f_{n+1}^k(x) = f_n^k(x) + b_k \cdot 2^n$ mit $b_k \in \{0, 1\}$. Es folgt

[1] Diese Behauptung gilt auch für $n = 1$.

durch zweifache Anwendung der Induktionsvoraussetzung sowie Behauptung 1

$$\begin{aligned} f_{n+1}^{2^{n-1}}(x) &= f_{n+1}^{2^{n-2}} \circ f_{n+1}^{2^{n-2}}(x) = f_{n+1}^{2^{n-2}}(x + 2^{n-1} + b_{2^{n-2}} \cdot 2^n) \\ &= f_{n+1}^{2^{n-2}}(x) + 2^{n-1} + b_{2^{n-2}} \cdot 2^n = x + 2^{n-1} + b_{2^{n-2}} \cdot 2^n + 2^{n-1} + b_{2^{n-2}} \cdot 2^n \\ &= x + 2^n. \end{aligned}$$

□

Die gesuchte Aussage folgt nun nochmal mittels Induktion. Für $n = 2$ erhalten wir die Periode $1 \mapsto 3(\mapsto 1)$ der Länge 2.
Sei $a_1, \ldots, a_{2^{n-1}}$ eine Periode von f_n und $a'_1, \ldots, a'_{2^n}$ die entsprechende Folge in $(\mathbb{Z}/2^{n+1})^*$ mit $a'_1 = a_1$ und $a'_{i+1} = f_{n+1}(a'_i)$ für $1 \leqslant i \leqslant 2^n - 1$. Dann gilt $a'_i = a_i + b_i \cdot 2^n$ für gewisse $b_i \in \{0, 1\}$ und $1 \leqslant i \leqslant 2^{n-1}$. Offensichtlich sind die a'_i für $i \leqslant 2^{n-1}$ paarweise verschieden, da $a'_i \bmod 2^n = a_i \neq a_j = a'_j \bmod 2^n$ für alle $1 \leqslant i < j \leqslant 2^{n-1}$. Nach Behauptung 2 gilt $a'_{i+2^{n-1}} = a'_i + 2^n$, sodass sogar für alle $1 \leqslant i \leqslant 2^n$ die a'_i paarweise verschieden sind. Damit erhalten wir wie gefordert eine Periode der Länge 2^n.

Bemerkung. Alle bis Mittwoch, 20.01.2016, 16:15, eingereichten Lösungen, waren richtig. Die Autoren erhalten jeweils einen Notenbonus von 0,3. Die Lösungen können in der Zentralübung abgeholt werden.

Aufgabe 40

Wir wissen, dass $|p - q| \leqslant 2^{m-7}$ mit $m = 256$. Setzt man $p = N/q$, so erhält man eine quadratische Ungleichung $q^2 + 2^{m-7}q - N \geqslant 0$ und somit

```
q_min := 97_30859_50955_56723_45764_58615_93865_81040_02215_
         08908_70677_81113_41255_39828_37426_64817
```

Implementiert man den fermatschen Faktorisierungsalgorithmus, z.B. mit `aribas`

```
function fer_factorize(N:integer):array;
external
q_min;
var
k,n:integer;
y:real;
v:array[2];
begin
n:=floor(sqrt(N))+1;
for k:=0 to n-q_min do;
y:=sqrt((n+k)**2-N);
if floor(y)=y then v[0..1]:=(n+k+floor(y),n+k-floor(y));
return v;
break;
end;
end;
end.
```

so erhält man

```
p = 97_75986_15749_30740_42230_55319_04247_90930_43816_
    93187_16548_38138_45070_38229_99439_55923,
q = 97_75986_15749_30740_42230_55319_04247_90928_88374_
    85497_78169_36919_46597_28393_56742_85603.
```

Sei $\varphi(N) = (p-1)(q-1)$, dann erhalten wir mit der `aribas`-Funktion `gcdx` d, v mit $de+v\varphi(N) = 1$.

```
==> gcd(e,vp,d,v); d.
-: 8217_57985_01114_08498_32446_37992_88579_22416_28290_78511_04397_69513_
34095_80135_85245_83312_54710_55380_23319_65588_25424_46097_32875_25029_19491_
49522_09986_45888_82917_14196_55297
```

Nun können wir den Geheimtext y mittel $y^d \bmod N$ in den Klartext

```
13_99613_83750_05971_69498_18674_83662_69019_62523_53958_53853_46302_51723_
17530_77612_13968_44971_36816_54183_15330_75071_78297_17822_20362_64900_34973_
27627_89120_51546_91550_71092
```

umwandeln. Umwandlung ist `Ascii`-Zeichen liefert

```
x:=y**d mod N;
b:=byte_string(x);
mem_byteswap(b,length(b));
string(b).
```

wobei `mem_byteswap` entsprechend der Vorgabe $x = \sum_{i=1}^{n} a_i 2^{n-i}$ die Reihenfolge der `length(b) = 63` Bytes in b umkehrt. Wie erhalten den Hinweis:

```
Die Klausur findet am 08.02.2016, 16-18 Uhr, im Raum C123 statt
```