BERZSENYI DÁNIEL TANÁRKÉPZŐ FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI VIII.
TERMÉSZETTUDOMÁNYOK 3.
Szombathely, 1992. 71–91.

SZALAY LÁSZLÓ

EGY DISZKRÉT ITERÁCIÓ A SZÁMELMÉLETBEN

Abstract:
Szalay L.: 1992., A discreten iteration in number theory. Tud. Közl. Szombathely, Természettudományok 3. 71–91.

Some years ago a detailed analysis was made by professor Francois Robert and his co–workers on the discrete (and continuous) iterations. The mathematical theory was worked out, and a lot of fields were found, such as: theoretical computer science, biomathematics, physics, sociology and psychology, where the discrete iterative scheme can be applied to the modelling of certain problems.

The present work discusses the

$$x_{n+1} \equiv x_n^2 \bmod M$$

special discrete iteration, with particular emphasis on the investigation of the iteration graphs' structures. The matter of producing iteration graphs is also discussed.

1. fejezet

1.1. Alapfogalmak.

Diszkrét iteráció:
Legyen X véges halmaz,
F az X–et önmagába vivő leképezés ($F:X \to X$),
$x_o \in X$ kezdőelem.

Tekintsük a következő iterációt:

$$x_{r+1} = F(x_r) \qquad (r= 0, 1, 2, \ldots).$$

Az egymás után végrehajtott iterációs lépések egy sorozatot generálnak, melynek a viselkedését vizsgáljuk.

Mivel X véges halmaz, a sorozat tetszőleges x_0 kezdőelem esetén periodikussá válik. Alapvetően két különböző típus lehetséges.

* Néhány kezdeti lépés után egy $t \in X$ állandóvá válik:
$F(t) = t$. Ekkor t elnevezése fixpont.

** Valamikor egy korábbi elemet kapunk vissza:

$$F(t_1) = t_2$$
$$F(t_2) = t_3$$
$$\ldots\ldots\ldots\ldots$$
$$F(t_n) = t_1 \quad (t_1, t_2, \ldots, t_n \text{ különbözők})$$

Ekkor $(t_1, t_2, \ldots, t_n)$-t n elemű ciklusnak hívjuk.
A fixpont és a ciklus közös elnevezése: attraktor.

Iterációs gráf:
- irányított,
- csúcsai az X halmaz elemei,
- él vezet x-ből y-ba, ha $F(x) = y$.

1.2. Az iteráció

Legyen M tetszőleges egynél nagyobb természetes szám: modulus. Az X alaphalmaz elemei a mod M maradékosztályok.
Vegyük az alábbi $F:X \to X$ leképezést: minden x_i maradékosztályhoz rendeljük hozzá az $x_i x_i$ maradékosztályt, azaz

$$x_{i+1} = F(x_i) = x_i x_i$$

Például M=9 esetén

x	0	1	2	3	4	5	6	7	8
F(x)	0	1	4	0	7	7	0	4	1

Három összefüggő részgráf látható. Két fixpont van: 0; 1, valamint egy db. kételemű ciklus: (4, 7).

Az iterációs gráf szerkezetét vizsgálva a továbbiakban szó lesz:
- fixpontokról,
- ciklusokról,
- szimmetriaviszonyokról a gráfon belül,
- bináris fákról,
- illetve attraktorkereső és gráfrajzoló algoritmusról.

1.3 Attraktorkereső algoritmusok

Az attraktorok számítógépes keresésének természetszerű módja a következő eljárás. A kiindulási x_0 maradékosztályt egy tömb elejére tesszük.Az újonnan előállított maradékosztályokat is folyamatosan ebben a tömbben tároljuk. Az új elemet összehasonlítjuk a már tömbben levőkkel. Amennyi-

ben találunk vele egyezőt, a kettő közti tömbelemeket kinyomtatjuk. A futás hosszabb időt vehet igénybe, ha M nagy.

D. HOFFMANN és *L. MOHLER* egy másik, gyorsabb attraktorkereső algortimust adtak, amely csak két memóriahelyet foglal a részadatok tárolására. (RHOP–algoritmus). A két változó, amelyre szükség van: Slow és Fast. Kezdetben mindkét változó a kiindulási x_o értéket kapja. Az iterativ ciklusban 3 utasítás van:

Fast:=F (Fast),
Fast:=F (Fast),
Slow:=F (Slow).

Látható, hogy a Fast változó kétszer olyan gyorsan mozog az attraktor felé, majd köröz abban, mint a Slow. Az attraktorban Fast utoléri Slow–t, ekkor ér véget a ciklus. Az elemek azonosítására a Slow aktuális értékéből kiindulva még néhányszor végrehajtjuk az iterativ lépést úgy, hogy Slow járja végig az attraktort, és a közbeeső értékeket írja ki. Az összes attraktor megkereséséhez többször kell alkalmazni a RHOP–eljárást.

2. fejezet

Vizsgálandó, hogy adott M modulus esetén hány fixpont van és melyek ezek.

Triviális fixpont lesz a t=o és a t=1 maradékosztály tetszőleges M esetén. Az iterációs gráfban tehát legalább 2 fixpont és az ezekhez tartozó összefüggő részgráf szerepel. Van–e még fixpont? A kérdés megválaszolására az

(1) $x^2 \equiv x \bmod M$

másodfokú kongruenciát kell megoldani.

2.1 $M=10^k$ speciális eset ($k > 0$ természetes szám).

(1)–vel ekvivalens az

(2) $x(x-1) \equiv 0 \bmod 10^k$

kongruencia. A két triviális fixpont rögtön adódik: $x \equiv 0$, $x \equiv 1$.
Mivel $(x, x-1) = 1$ ezért nem triviális fixpontot kapunk az

$$\text{(3)} \quad \begin{array}{ll} x \equiv 0 & \bmod 2^k \\ x-1 \equiv 0 & \bmod 5^k, \end{array}$$

majd az

$$\text{(4)} \quad \begin{array}{ll} x \equiv 0 & \bmod 5^k \\ x-1 \equiv 0 & \bmod 2^k \end{array}$$

szimultán kongruenciarendszerek megoldásával. Ezek megoldhatók és egy-egy megoldásuk lesz mod $[2^k, 5^k] = 10^k$ modulusra nézve:

(3) megoldása: $x_1 \equiv \left(2^k\right)^{\varphi(5^k)} \mod 10^k$

(4) megoldása: $x_2 \equiv \left(5^k\right)^{\varphi(2^k)} \mod 10^k$

(Euler kongruenciatétele alapján könnyen belátható, hogy ezek valóban megoldások).

A fentiekből következik, hogy $M=10^k$ esetén pontosan 2 nem triviális fixpont lesz k–tól függetlenül, k–tól a megoldások függnek. Például:

k	1	2	3	4	5	6
x_1	5	25	625	0625	90625	890625
x_2	6	76	376	9376	09376	109376

A kiszámított nem triviális fixpontok érdekessége (*TÉDENANT, M.* 1814–15):

- adott k esetén $x_1+x_2 = 10^k+1$,
- k–ról k+1–re lépve mindig egy új számjegy kerül a korábbi x_1 ill. x_2 elé.

Általános M modulus mellett is igaz lesz: ha x fixpont, akkor M+1–x is az, a fixpontok párokban fordulnak elő. (Meggondolható, hogy egyik fixpont sem lehet önmaga párja.)

2.2. Általános eset

Legyen $M=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ $(p_i \neq p_j$ ha $i \neq j)$
továbbá $k > 0$ természetes szám. Oldjuk meg az

(5) $$x^2 \equiv x \mod M^k$$

kongruenciát. Vele ekvivalens:

(6) $$x(x-1) \equiv 0 \mod M^k$$

(a két triviális megoldás: $x\equiv 0$ ill. $x\equiv 1 \mod M^k$)

$(x, x-1) = 1$ miatt egy fixpontot kapunk, ha képezzük a következő szimultán kongruenciarendszert:

$$x\equiv 0 \mod m_1^k$$
$$x\equiv 1 \mod m_2^k,$$

ahol $(m_1, m_2) = 1$ és $m_1 m_2 = M$. Pontosan egy megoldás van mod $[m_1^k, m_2^k]=M^k$ modulusra:

(7) $$x\equiv \left(m_1^k\right)^{\varphi(m_2^k)} \mod M^k$$

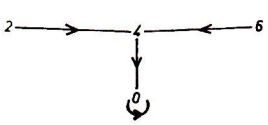
M^k egy „felbontása" során 1 megoldás van. Az összes megoldást megkaphatjuk, ha minden lehetséges módon felírjuk M^k–t két egymáshoz

relativ prim szorzatára a sorrendet is figyelembe véve. M különböző primosztóinak száma: s, amiből az összmegoldásszám: 2^s (a két triviális megoldást akkor kapjuk, ha $m_1=1$ vagy $m_2=1$).

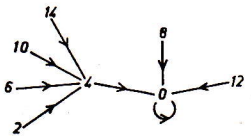
A fixpontok száma független k-tól, csak a megoldások függenek tőle. Adott M mellett A_1-gyel jelölve a fixpontok számát $A_1=2^s$.

Megjegyzések:

- M prim vagy primhatvány, akkor és csak akkor két fixpont lesz (0,1). (*1., 2., 3., 4. ábra*),

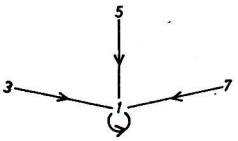


M = 16

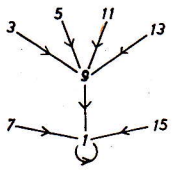


M = 16

M = 8

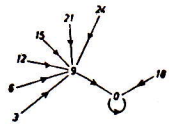


1. ábra



2. ábra

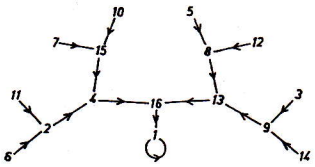
M=27



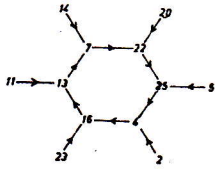
M=17

M=27

M=17



M=27

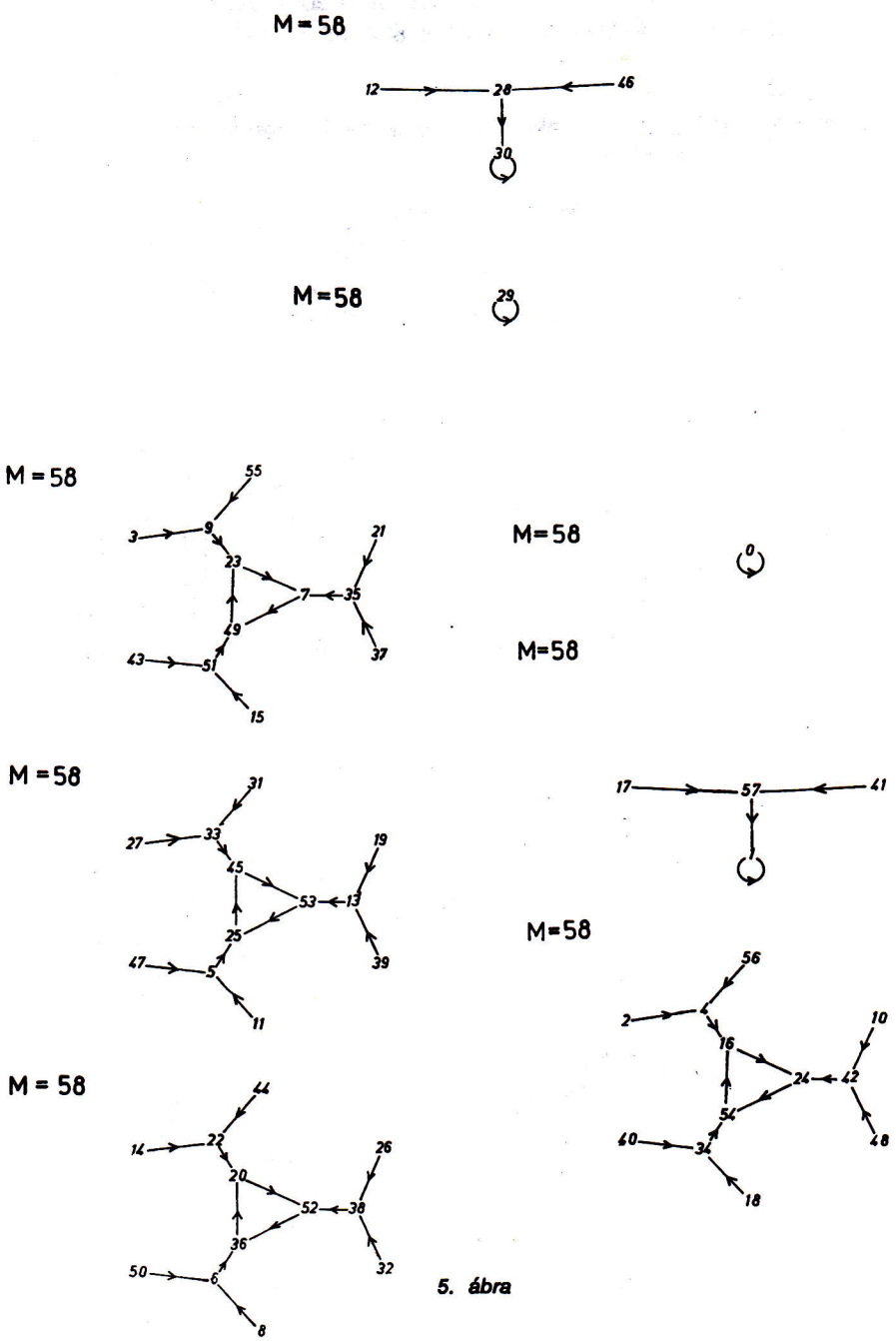


M=27

3. ábra

4. ábra

– M=2P, ahol P páratlan szám, akkor egyik fixpontpár: p, p+1. (A másik a triviális.) (*5. ábra*),



5. ábra

– szemléletes jelentése az eddigieknek: Ha M alapú számrendszerben olyan számokat keresünk, melyek utolsó k jegye megegyezik a szám négyzetének utolsó k jegyével, akkor az ilyen k-jegyű végződések száma 2^s db lesz, a számok (7)-ből adódnak.

2.3. Következmények.

Euler kongruenciatétele nem ad felvilágosítást azon esetről, mikor a modulus és a hatványalap nem relatív primek. A következő két tétel az általános esetről ad felvilágosítást.

1. TÉTEL:

Ha $a^{\varphi(M)} \equiv t \bmod M$ akkor t az $x^2 \equiv x \bmod M$ egy megoldása.

(azaz $\left(a^{\varphi(M)}\right)^2 \equiv a^{\varphi(M)} \bmod M$)

BIZONYÍTÁS:

Ha (a, M) =1 akkor $a^{\varphi(M)} \equiv 1 \bmod M$; $1^2 \equiv 1 \bmod M$.

Ha a= BM akkor $a^{\varphi(M)} \equiv 0 \bmod M$; $0^2 \equiv 0 \bmod M$.

Ha a fenti két eset egyike sem teljesül, akkor tegyük fel, hogy (a, M)=d (1<d<M). Legyenek $p_1, p_2, \ldots, p_s$ rendre azon primek, melyek M és a primfelbontásában is szerepelnek, rajtuk kívül több ilyen nincs. Eszerint

$$M = (r_1^{\gamma_1} r_2^{\gamma_2} \ldots r_t^{\gamma_1})\,(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}) = M' \cdot d_1 \quad ((M', d_1) = 1),$$

$$a = (p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s})\,(q_1^{\delta_1} q_2^{\delta_2} \ldots q_u^{\delta_u}) = d_2 \cdot a' \quad ((d_2, a') = 1).$$

Így teljesülnek a következők is:

$$(M', a')=1;\ (M', a)=1;\ (M, a')=1;\ \varphi(M) = \varphi(M')\,\varphi(d_1)$$

A tétel bizonyításához elég belátni, hogy

(a) $(a^{\varphi(M)})^2 \equiv a^{\varphi(M)} \bmod M'$

(b) $(a^{\varphi(M)})^2 \equiv a^{\varphi(M)} \bmod d_1$

(a) $(a^{\varphi(M)})^2 = (a^{\varphi(M')\,\varphi(d_1)})^2 = (a^{2\varphi(d_1)})^{\varphi(M')} \equiv 1 \bmod M'$

$a^{\varphi(M)} = (a^{\varphi(d_1)})^{\varphi(M')} \equiv 1 \bmod M'$

(b) Belátjuk, hogy $a^{\varphi(M)} \equiv 0 \bmod d_1$. Ehhez elég megmutatni, hogy $d_1 \mid a^{\varphi(d_1)}$, de elég már $d_1 \mid d_2^{\varphi(d_1)}$-t bizonyítani.

Mivel $d_2^{\varphi(d_1)} = \prod_{i=1}^{s} p_i^{\beta_i \varphi(d_1)}$ így a feladat $\alpha_i \le \varphi(d_1)$ igazolása

$$\varphi(d_1) = \prod_{i=1}^{s} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right).$$

Ha bebizonyítjuk, hogy, $\alpha_i \leq p_i^{\alpha_i}(1-\frac{1}{p_i})$ akkor készen vagyunk. Az egyenlőtlenség jobb oldala akkor a legkisebb, ha $p_i=2$, ezért a következő állítás marad: $\alpha_i \leq 2^{\alpha_i - 1}$ amely nyilvánvaló.

2. TÉTEL:

Ha t_j az $x^2 \equiv x \bmod M$ kongruencia megoldása, akkor létezik $0 \leq a \leq M$ természetes szám, melyre $a^{\varphi(M)} \equiv t_j \bmod M$.

BIZONYÍTÁS:

Az $x^2 \equiv x \bmod M$ másodfokú kongruenciának mindig van két triviális megoldása, ezekhez az $a=0$ ill. az $a=1$ választással találhatunk megfelelő a–t. Ha van nem triviális megoldás, az a korábbiak szerint felírható

$$t_j \equiv m_1^{\varphi(m_2)} \bmod M$$

alakban, ahol $M = m_1 m_2$; $(m_1, m_2)=1$; $m_1, m_2 > 1$.

Bizonyítani kell, hogy létezik olyan a, melyre $a^{\varphi(M)} \equiv m_1^{\varphi(m_2)} \bmod M$. Lássuk be azt, hogy az $a=m_1$ választás megfelelő, vagyis $m_1^{\varphi(M)} \equiv m_1^{\varphi(m_2)} \bmod M$. Vele ekvivalens kongruenciarendszer:

$$(m_1^{\varphi(m_2)})^{\varphi(m_1)} \equiv m_1^{\varphi(m_2)} \bmod m_1,$$
$$(m_1^{\varphi(m_1)})^{\varphi(m_2)} \equiv m_1^{\varphi(m_2)} \bmod m_2,$$

és mindkét állítás egyszerűen belátható (a második az Euler tétel következménye).

Összefoglalva: Ha $a^{\varphi(M)} \equiv t_j \bmod M$ akkor t_j az $x^2 \equiv x \bmod M$ egy megoldása, és ha a végigmegy a 0, 1, 2, ..., M–1 számokon akkor az $x^2 \equiv x$ minden megoldását megkapjuk.

3. fejezet

A többelemű attraktorok vizsgálatához szükség lesz az alábbi állításra *(KISS P. 1978)*.

Az $x^k \equiv x \bmod p_i^{\alpha_i}$ megoldásszáma és megoldásai:

$p_i=2$ esetén

ha $\alpha_i = 1$ akkor 2 megoldás: $x \equiv 0$; $x \equiv 1 \bmod 2$,

ha $\alpha_i > 1$ akkor $1 + (k-1, 2)\cdot(k-1, 2^{\alpha_i - 2})$ db megoldás:

$$x \equiv 0;\ x \equiv (-1)^{cq} 5^{c_1 q_1} \bmod 2^{\alpha_i},$$

ahol $c = \frac{2}{(k-1, 2)}$; $c_1 = \frac{2^{\alpha_i - 2}}{(k-1, 2^{\alpha_i - 2})}$

és $0 \leq q < (k-1, 2)$; $0 \leq q_1 < (k-1, 2^{\alpha_i - 2})$

$p_i > 2$ prim estén

$1+ (k-1 , \varphi(p_i^{\alpha_i}))$ db megoldás:

$x \equiv 0 ; x \equiv g_i^{c_i q_i} \bmod p_i^{\alpha_i}$, ahol

$$c_i = \frac{\varphi(p_i^{\alpha_i})}{(k-1, \varphi(p_i^{\alpha_i}))} ; 0 \le q_i < (k-1, \varphi(p_i^{\alpha_i}))$$

és g_i egy primitiv gyök mod $p_i^{\alpha_i}$.

3.1 Kételemű attraktorok

Az $y \in X$ elem akkor lesz egy kételemű attraktor egyik tagja, ha teljesül rá, hogy $y = F(F(y))$ és $y \neq F(y)$ (azaz nem fixpont). Konkrétan:

(8)
$$\text{(a) } x^4 \equiv x \bmod M,$$
$$\text{(b) } x^2 \not\equiv x \bmod M.$$

Keressük (8/a)-t kielégítő maradékosztályok számát. Jelöljük ezt M_2-vel. A_2-vel a kételemű attraktorok és a továbbiakban A_i-vel az i elemű attraktorok számát. Egy attraktort elég egy elemével azonosítani, ezért

$$A_2 = \frac{M_2 - A_1}{2}$$

Legyen $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ és keressük M_2-t. (8/a)-val ekvivalens az alábbi kongruenciarendszer:

(9)
$$x^4 \equiv x \bmod p_1^{\alpha_1}$$
$$x^4 \equiv x \bmod p_2^{\alpha_2}$$
$$\ldots\ldots\ldots\ldots$$
$$x^4 \equiv x \bmod p_s^{\alpha_s}$$

Alkalmazzuk most a fejezet elején említett állítást. Ha a 2 szerepel M primtényezői között, két megoldása ($x \equiv 0$; $x \equiv 1$) lesz (9) megfelelő kongruenciájának ($\alpha_i = 1$ esetén triviális, $\alpha_i > 1$ esetén pedig $(k-1, 2^{\alpha_i - 2}) = (3, 2^{\alpha_i - 2}) = 1$ miatt).

Válasszuk ki valamelyik primtényezőt: p_i , és nézzük (9) rá vonatkozó kongruenciáját. Legyen $T = (3, \varphi(p_i^{\alpha_i}))$

(a kiválasztott kongruencia megoldásainak száma: T+1). T lehetséges értékei: 1 ill. 3, arra szeretnénk feltételt megfogalmazni, hogy ez mitől függ. $\varphi(p_i^{\alpha_i}) = (p_i - 1) p_i^{\alpha_i - 1}$, tehát T=3 akkor lehetséges, ha

$3 \mid p_i - 1$, vagyis $p_i = 6k+1$ alakú prim, vagy

$3 = p_i$ és $\alpha_i > 1$.

Tegyünk különbséget M primfelbontásában levő primek között.

$M = 2^{\alpha}3^{\beta}\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$ ahol

p_i : 6k+1 alakú prim; q_j : 6k+5 alakú prim; $\alpha, \beta \geq 0$;

$\alpha_i, \beta_i > 0$ továbbá s a különböző primosztók száma.

Ha $\beta=0$ vagy $\beta=1$ akkor $M_2 = 2^{s-r}\, 4^r$

Ha $\beta>1$ akkor $M_2 = 2^{s-r-1}\, 4^{r+1}$.

Tehát $$A_2 = \begin{cases} 2^{s+r-1} - 2^{s-1} & \beta<2 \text{ esetén} \\ 2^{s+r} - 2^{s-1} & \beta>1 \text{ esetén} \end{cases}$$

E képlet megadja a kételemű attraktorok számát, az attraktorok meghatározása a fejezet elején említett állítás felhasználásával történhet. Az első néhány modulus, amikor már előfordul kételemű ciklus:

M	7	9	13	14	18	19	21	26	27	28	31	35	36
A_2	1	1	1	2	2	1	2	2	1	2	1	2	2

(az iterációs gráfok megtalálhatók: ~~Melléklet~~ 4. ábra).

3.2 Speciális többelemű attraktorok

Vizsgáljuk bizonyos speciális w hosszúságú ciklusok számát. A specialitás abban áll, hogy legyen 2^w-1 prim (Mersenne–prim). Ha valamely x elem egy w hosszú ciklus része, akkor $F^w(x)=x$ teljesül ennek megfelelően:

(10) $$x^{2^w} \equiv x \bmod M$$

Ki kell zárni, hogy

– x fixpont legyen: $x^2 \not\equiv x \bmod M$,

– olyan d< w elemű attraktor része legyen, melyre d|w , tehát $x^{2^d} \not\equiv x \bmod M$.

A kizárás egyszerű, ha w prim, ekkor csak a fixpontvizsgálattal kell foglalkozni. Legyen most w prim és adjuk meg $x^{2^w} \equiv x \bmod M$ megoldásszámát. Részekre bontva:

(a) $x \equiv 0 \bmod M$,

(11) (b) $x^{2^w-1} \equiv 1 \bmod M$.

(11/b)–nél meg kellene vizsgálni M különböző primhatványainak és 2^w-1-nek a legnagyobb közös osztóját. Ez bonyolult lehet általános esetben de egyszerű, ha 2^w-1 prim. Így indokolható a kezdetben alkalmazott szelekció.

Legyen $M = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_s^{\alpha s}$; $T = \left(2^w-1,\ \varphi\left(p_i^{\alpha_i}\right)\right)$

$x^{2^w-1} \equiv 1 \bmod p_i^{\alpha_i}$ megoldásainak száma: 2 ha T=1
2^w ha $T=2^w-1$

$T=2^w-1$ lehetséges, ha
$p_i = (2^w-1)k+1$ alakú prim vagy
$p_i = 2^w-1$ és $\alpha_i > 1$

Legyen $M=2^{\alpha}\,(2^w-1)^{\beta}\,p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}q_1^{\beta_1}q_2^{\beta_2}\ldots q_t^{\beta_t}$ ahol

p_i: $(2^w-1)k+1$ alakú prim; q_i: nem $(2^w-1)k+1$ alakú prim;
$\alpha_i, \beta_i > 0$; $\alpha, \beta \geq 0$ valamint M különböző primosztóinak száma s.
Ha $\beta=0$ vagy $\beta=1$ akkor $M_w=2^{s-r}\,(2^w)^r$
Ha $\beta>1$ akkor $M_w = 2^{s-r-1}\,(2^w)^{r+1}$

Így $$A_w = \begin{cases} \dfrac{2^s(2^{(w-1)r}-1)}{w} & \text{ha } \beta < 2 \\ \dfrac{2^s\left(2^{(w-1)(r+1)}-1\right)}{w} & \text{ha } \beta > 1. \end{cases}$$

E képlet megadja a w hosszúságú attraktorok számát, ha 2^w-1 prim (w= 2, 3, 5, 7, 13, ...). Például w=3 esetén (*5. ábra*).

M	29	43	49	58	71	86	87	98	113	116
A_3	2	2	2	4	2	4	4	4	2	4

3.3 Tetszőleges hosszú ciklusok

A 3.2 alfejezet elején sikerült megfogalmazni, hogy mikor tekintünk egy X–beli elemet egy w hosszúságú ciklus részének. Akkor w specialitását kihasználva adtunk képletet A_w-re. Ilyen képlet általánosságban nehezen adható, de egy egyszerű, bár kevésbé használható viszont igen. Jelöljük A_d-vel a d elemű attraktorok számát, M_w–vel pedig (10) megoldásszámát.

$$A_w = \frac{M_w - A_1 - \sum_{\substack{d \mid w \\ 1<d<w}} d\,A_d}{w}$$

megadja a w elemű attraktorok számát (*4. ábra*), de ismerni kell hozzá minden d | w esetén a d elemű ciklusok számát (A_d).

4. fejezet

A szimmetria értelmezése

Az M modulushoz tartozó irányított gráfot szimmetrikusnak nevezzük, ha az összefüggő részgráfok halmaza két részre osztható úgy, hogy a két halmaz között létezik olyan bijekció, hogy az egymáshoz rendelt részgráfok izomorfak. (*2., 5. ábra*).

Csak az M páros esettel foglalkozunk, hiszen M páratlan esetén eleve nem lehet szimmetrikus a gráf. Ha M páros, akkor az iteráció paritástartó, ami bizonyos megosztottságra utal. Rögzítsük le M-t és tegyük fel, hogy létezik olyan b szám, melyre minden $x^2 \equiv y \bmod M$ esetén $(x+b)^2 \equiv y+b \bmod M$. Ez azt jelentené, hogy bármely x kezdőelemből indulunk ki és hajtjuk végre az iterációs lépéseket, a kapott alakzatról készül egy *„másodpéldány"*, melynek elemeit megkapjuk, ha az első sorozat megfelelő elemeihez b-t adunk. Például M=6 esetén b=3. Mikor létezik megfelelő b?

Vonjuk ki egymásból az alábbi két kongruenciát:

$$(x+b)^2 \equiv y+b \bmod M$$
$$x^2 \equiv y \bmod M$$
$$2bx+b^2 \equiv b \bmod M \qquad (12)$$

(12) teljesül ha (13) mindegyike teljesül.

$$2bx \equiv 0 \bmod M$$
$$b^2 \equiv b \bmod M \qquad (13)$$

(13) első fele rögzített b esetén megoldható. A második fele igaz, ha b fixpont. Tehát olyan fixpontot kell keresni, melyre minden x esetén $2bx \equiv 0 \bmod M$ is teljesül.

TÉTEL:

Ha $M=2^{\alpha} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}$ és $\alpha=1$ vagy $\alpha=2$ akkor létezik megfelelő fixpont, tehát M-hez tartozó iterációs gráf szimmetrikus.

A bizonyítást két részletben végezzük.

$\alpha = 1$

A 2.2 fejezet második megjegyzése szerint M/2 fixpont. Ha $x^2 \equiv y \bmod M$, akkor $(x+\frac{M}{2})^2 = x^2+Mx+\left(\frac{M}{2}\right)^2 \equiv y+\frac{M}{2} \bmod M$, a „távolságtartás" öröklődik. A gráf szimmetrikus lesz.

$\alpha = 2$

Először lássuk be, hogy

ha $\frac{M}{4} = 4k+1$ alakú, akkor $\frac{M}{4}$ fixpont,

ha $\frac{M}{4} = 4k+3$ alakú, akkor $\frac{3M}{4}$ fixpont

A bizonyításuk:

$$\frac{M}{4}\,\frac{M}{4} = (4k+1)\,\frac{M}{4} = kM + \frac{M}{4} \equiv \frac{M}{4} \bmod M$$

$$\left(\frac{3M}{4}\right)\left(\frac{3M}{4}\right) = \left(\frac{9M}{4}\right)\frac{M}{4} = \frac{9M}{4}(4k+3) = 9kM + \frac{27}{4}M \equiv \frac{3}{4}M \bmod M$$

A következő lépés a *„távolságtartás"* öröklődésének megmutatása. Legyen x tetszőleges páros elem ($0 \leq x \leq M$). Ezt megtehetjük, mivel paritástartó az iteráció, és így a bijekció a páros elemeket tartalmazó részgráfhoz páratlanokat tartalmazót fog hozzárendelni.

Ha M/4 $4k+1$ alakú: $\left(x + \frac{M}{4}\right)^2 = x^2 + M\frac{x}{2} + \left(\frac{M}{4}\right)^2 \equiv y + \frac{M}{4} \bmod M$

Ha M/4 $4k+3$ alakú: $\left(x + \frac{3M}{4}\right)^2 = x^2 + M\frac{3x}{2} + \left(\frac{3M}{4}\right)^2 \equiv y + \frac{3M}{4} \bmod M$

A $b = M/4$ vagy $b = 3M/4$ választással megfelelő fixpontot kapunk, az iterációs gráf szimmetrikus lesz.

Mi van $\alpha > 2$ esetén? Az előző típusú bizonyítás nem működik, mert $\frac{M}{2^\alpha}(2i+1)$-k között ($i=0, 1, 2, \ldots$) nem található megfelelő fixpont. A számítógépes vizsgálatok szerint ha M osztható 8-cal, akkor néha szimmetrikus lesz az iterációs gráf, néha nem. Külön érdekesség, hogy ilyen esetekben a szimmetria teljesen más típusú, mert nem teljesül a *„távolságtartás"* (*2. ábra*). A nem szimmetrikus eseteknél (*1. ábra*) a gráf majdnem szimmetrikus, valami *„apróságon"* bukik el.

5. fejezet

Tetszőleges M modulus mellett legalább két fixpont van, ezért az iterációs gráf sosem lesz összefüggő. Az 1-be mindig fut be él ((M–1)-ből), a nulláról ugyanez nem mondható el.

Bináris fa értelmezése

Az iterációs gráfot bináris fának nevezzük, ha két összefüggő részgráfból áll, és teljesülnek az alábbiak:

- a 0 izolált fixpont,
- az 1 fixpontba egy él fut be ((M–1)–ből),
- az (M–1)–be és a leveleken kívül minden további csúcsba két másik él fut be. *(3. ábra).*

A bináris fa létezésének szükséges feltétele könnyen megfogalmazható. Mivel csak a triviális fixpontok vannak, ebből következik, hogy M prim vagy primhatvány. Amennyiben M prímhatvány ($M=p^t$, p prím, $t > 1$), akkor a 0 nem lesz izolált fixpont, mert $(p^{t-1})^2 \equiv 0 \bmod p^t$. Ha M=p prím és p–1-nek van páratlan prímosztója, akkor van benne kör, ugyanis található olyan $w>0$ és x (x nem fixpont) amelyekre $x^{2^w} \equiv x \bmod p$, tehát $M=2^t+1$ alakú kell, hogy legyen. A jelenleg ismert Fermat–prímek: 2, 3, 5, 17, 257, 65537. Az M=2 eset nem bináris fát határoz meg, a többi

$2^{2^n} + 1$ alakban írható.

A 3, 5, 17, 257 ellenőrizhető: valóban bináris fa lesz az általuk meghatározott gráf. Az M=65537 esetet még számítógéppel is lehetetlennek tűnik kirajzoltatni, a további esetleges Fermat–prímekkel ugyanez a helyzet.

Bináris fa létezésének szükséges és elégséges feltétele:

$M=2^{2^n}+1$ alakú prím legyen.

BIZONYÍTÁS:

A szükséges feltételt már beláttuk korábban, következik az elégséges feltétel. Bizonyítani kell:

(a) a 0 izolált fixpont,

(b) minden elemnek van egy párja és csak ők ketten futnak egy bizonyos csúcsba,

(c) a 0–n kívül bárhonnan el lehet jutni az 1–be az éleken keresztül,

(d) a levelek száma is kettő hatványa.

A négy részbizonyítás:

(a) $x^2 \equiv 0 \bmod M$ kongruenciának egy megoldása van:
$x \equiv 0 \bmod M$ (minden primmodulusra igaz).

(b) x_1 elem párja az $(M-x_1)$ lesz, mert ha $x_1^2 \equiv y \bmod M$ akkor $(M-x_1)^2 \equiv y \bmod M$, és más elem nincs, melynek négyzete y–nal volna kongruens. Ugyanis ha $x_2^2 \equiv y \bmod M$ teljesül, ebből $(x_1-x_2)(x_1+x_2) \equiv 0 \bmod M$ következne. Mivel M prim, ezért a lehetséges esetek:
vagy $x_2 \equiv x_1 \bmod M$,
vagy $x_2 \equiv -x_1 \bmod M$ (tehát (b) is minden primre igaz).

(c) Ha $x \equiv 0 \bmod 2^{2^n}+1$ akkor tetszőleges x–hez létezik olyan r természetes szám, hogy $x^{2^r} \equiv 1 \bmod 2^{2^n}+1$. Az $r= 2^n$ megfelel, mert az

$$x^{2^{2^n}} \equiv 1 \mod 2^{2^n}+1$$

kongruencia megoldásszáma $(2^{2^n}, 2^{2^n}) = 2^{2^n}$, amely a nullán kívül az összes többi számot jelenti. (Itt már kihasználtuk M speciális prím voltát.)

(d) Az $M=2^{2^n}+1$ primhez $\frac{M-1}{2}$ db kvadratikus maradék van, és ugyanennyi kvadratikus nem maradék. Az $x^2 \equiv b \bmod M$ kongruenciának 2^{2^n-1} különböző b mellett lesz megoldása, a levelek száma is $2^{2^{n-1}}$. (Ismét fontos volt, hogy $M=2^{2^n}+1$ alakú prím.)

Eddigi ismereteink szerint 5 db bináris fa létezik: $M=2^{2^n}+1$ (n=0, 1, 2, 3, 4) modulusok esetén.

6. fejezet

Az attraktorkereső algoritmusokról az 1.3-ban volt szó. Nehezebb probléma egy olyan algoritmus megadása, amely az iterációs gráfot kirajzolja a képernyőre tetszőleges M modulus esetén.Egy ilyen leírása következik.

Az algoritmus általános, tetszőleges X halmaz és tetszőleges F leképezés esetén kirajzolja az iterációs gráfot (ha X elemei egyáltalán ábrázolhatók lesznek számítógépen, és az F leképezés eredménye kiszámolható). A képernyőn egyszerre 1 összefüggő részgráf látható, az iterációs gráf részenként jelenik meg.

Az algoritmus lényege:

A Rhop segítségével meghatározza az X halmaz egy attraktorát (természetesen egy attraktort csak egyszer). Az attraktor elemszámától függően szögtartományokra osztja a képernyőt. Ezután visszakeresi a közvetlenül az attraktorba futó elemeket, és tovább osztja a már meglevő szögtartományokat. A következő lépés további elemek visszakeresése, további képernyőosztás, stb. Ha egy részgráf minden elemét azonosította (IR=OLVAS) akkor a szögek és az attraktortól való távolság ismeretében (egyféle polárkoordináta rendszer) meghatározza a pontok koordinátáit a nagyfelbontású képernyőn, s összeköti a pontokat.

Az algoritmus pontos leírását a *melléklet* mutatja. Az ábrák bizonyítják az algoritmus helyességét, mivel azok egy Simon's Basic program futásának eredményei. A program az algoritmus kódolása.

Felhasznált fontosabb változók:

tömbök:

DATA (N–1) – az X halmaz elemeit tartalmazza,
A (N–1) – elemei természetes számok, ha A(I)=J,
akkor az X halmaz I–edik eleme a J–edikbe ment át
az F leképezéssel.
TMB (N–1) – segédtömb, amely egy attraktor és a hozzá kapcsolódó
X halmaz–beli elemek indexeit tartalmazza,
B(N–1) – logikai tömb, kezdetben minden eleme
FALSE, az I–edik eleme igazzá válik, ha az
X halmaz I–edik elemét már ábrázoltuk.
SZÖG1 (N–1) és,
SZÖG2 (N–1) – a képernyőre kerülő elemek szögtartományát
tartalmazzák,
KÖR (N–1) – az I–edik elem attraktortól való viszonylagos
távolságát jelzi,
KOORD1 (N–1) és KOORD2(N–2) az adott részgráf
képernyő koordinátáit tartalmazza.
változók:
N – X halmaz elemeinek száma,
ID – az attraktorkeresés az X halmaz ID–edik eleméből indul ki,
S1, S2 – a képernyő méretei,
SLOW, FAST – ld. 1.3 fejezet,
ADB – a megtalált attraktor elemszáma.

Az algoritmusban nem részletezett *„SZÁMKIIRÁS" és „EGYENES"* nevű eljárások az adott programozási nyelvnek megfelelően kiírják az elemeket a képernyőre, és berajzolják a gráf éleit.

BEFEJEZÉS

A vizsgált speciális iteráció érdekes szerkezetek megjelenéséhez vezetett, az iterációs gráfok sokszor esztétikai élményt is nyújthatnak.

Érdekes lenne szemügyre venni az általános másodfokú

$F(x) = ax^2+bx+c$

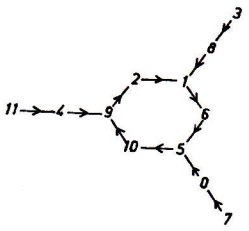
iterációt a mod M maradékosztályokra, vagy akár az n-edfokú

$F(x)= a_nx^n+... + a_1x+a_o$

iterációt. Ehhez készen áll a kutatást segítő algoritmus, amelyből könnyen használható program írható.

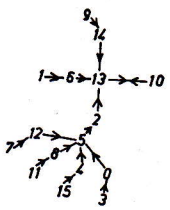
A *6., 7. ábrák* az $F(x) = x^3+5$ leképezés iterációs gráfjaiból mutatnak részleteket. Látható, hogy az eddig megszokott alakzatoktól eltérő gráfok is létrejöttek.

M = 12



6. ábra

M = 16



7. ábra

ALGORITMUS (X halmaz, N elem, F leképezés)

```
Ciklus I:=0-tól N-1-ig
    Be: DATA (I)
Ciklus vége
Ciklus I:=0-tól N-1-ig
    X:=F (DATA (I))
    J: = 0
    Ciklus amíg X<>DATA (J)
        J: = J+1
    Ciklus vége
    A(I): = J
    B(I) = FALSE
Ciklus vége
ID: =0
Ciklus amíg ID <N
    Ciklus amíg ID<N és B(ID)
            ID: = ID+1
    Ciklus vége
    Ha ID<N akkor TEVÉKENYSÉG
                  ID: ID+1
Ciklus vége
Algoritmus vége.
```

TEVÉKENYSÉG

```
SLOW: =A(ID)
FAST: = A (ID)
Ciklus
    FAST: = A(FAST)
    FAST: = A(FAST)
    SLOW: = A(SLOW)
amíg SLOW<>FAST
Ciklus vége
BÁZIS:=SLOW
SZÁML: =0
Ciklus
    SZÁML: = SZÁML+1
    SLOW: = A(SLOW)
    TMB (SZÁML) : = SLOW
amíg BÁZIS<>SLOW
Ciklus vége
ADB: = SZÁML
Ha ADB =1 akkor SZÖG1 (1): =150
                SZÖG2 (2) : = 390
                KÖR (1) : = 1
                SZÁML: = SZÁML+1
    Különben    RO: = 360/ADB
                KEZD: =RO/2
                Ciklus SZÁML: = 1-TŐL adb-IG
                  SZÖG1 (SZÁML): = KEZD+(SZÁML-1)RD
                  SZÖG2 (SZÁML): = SZÖG1 (SZÁML)+RO
                   KÖR (SZÁML): =1
                Ciklus vége
                SZÁML: = SZÁML+1
```

```
OLVAS: =1
IR: = SZÁML
Ciklus amíg OLVAS<>IR
    Ciklus I: =0-tól N-1-ig
        Ha A(I) = TMB (OLVAS) akkor J:=1
            Ciklus amíg J≤ ADB és I<>TMB (J)
                J: = J+1
            Ciklus vége
            Ha J>ADB akkor TMB (IR): =1
                IR: = IR+1
    Ciklus vége
    DB: = IR-SZÁML
    Ha DB<>0 akkor DELTA:=(SZÖG2 (OLVAS) - SZÖG1 (OLVAS))/DB
        Ciklus I: = SZÁML-tól IR-1-ig
            SZÖG1(I):=TMB (OLVAS)+ (I-SZÁML)DELTA
            SZÖG2 (I): = SZÖG1 (I)+DELTA
            KÖR (I): = KÖR (OLVAS)+1
        Ciklus vége
        SZÁML: = IR
    OLVAS: = OLVAS+1
Ciklus vége
KR: = KÖR (IR-1)
BX: = INT (S2/2) (S2: a képernyő szélessége)
BY: = INT (S1/2) (S1: a képernyő magassága)
Ha ADB = 1 akkor    KJEL: =1
                    Ha KR=1 akkor SUGÁR: = BX/KR
                        különben SUGÁR: =BX/(KR-1)
    különben        KJEL:=0
                    SUGÁR: =BX/KR
Ciklus I:=1-től IR-1-ig
    AVER:= (SZÖG1(I)+SZÖG2(I)/2
    TÁV:= (KÖR (I)-KJEL)SUGÁR
    KOORD1 (I):=TÁV COS (AVER)+BX
    KOORD2 (I):=TÁV SIN (AVER)+BZ
Ciklus vége
Ciklus I:= 1-től IR-1-ig
    B (TMB (I)):=TRUE
    C: = A(TMB(I))
    J:= 1
    Ciklus amíg C<> TMB (J)
        J:=J+1
    Ciklus vége
    SZÁMKIÍRÁS (TMB (I), KOORD1 (I), KOORD2 (I))
    EGYENES (KOORD1 (I), KOORD2 (I), KOORD1 (J), KOORD2 (J))

Ciklus vége

Tevékenység vége
```

IRODALOM

HOFFMANN D.–MOHLER L.: Mathematical Recreations for the Prgoram-mable Calculátor

KISS P. 1978.: Egy binom kongruenciáról – Az Egri Ho Si Mihn Tanárképző Főiskola füzetei, p. 459.–460.

ROBERT F. 1986.: Discrete iterations; Springer Series in Compatational Mathematics Vol. 6. Preprint

TÉDENANT M. 1814–1815.: Annales de Math., 5. p. 309–321.

A DISCRETE ITERATION IN NUMBER THEORY

The present study discusses a special discrete iteration which associates all M residue classes with its product with itself, if the M modul is fixed. By different moduls I investigate the structure of the iteration graph produced by the mapping.

Symbols:

s – the number of prime divisors of M

r – the number of prime divisors of M of the form 6k+1

t – the number of prime divisors of M of a form other than 6k+1

α – the exponent of 2 in the prime decomposition of M

β – the exponent of 3 in the prime decomposition of M

Assertions:

1. The number of fixed points: 2^s.

Fixed points: $x \equiv m_1^{\varphi(m_2)}$, where $m_1 m_2 = M$ and $(m_1, m_2)=1$, and we take all m_1, m_2 pairs.

2. If $a^{\varphi(M)} \equiv t \bmod M$, then t is a solution for $x^2 \equiv x \bmod M$, and if a takes the values 0, 1, 2, ..., M–1, then all solutions of the $x^2 \equiv x \bmod M$ arise in the form of $a^{\varphi(M)}$

(This is a generalization of Euler's congruency theorem.)

3. The number of binary cycles: $2^{s+r-1} - 2^{s-1}$ if $\beta<2$

$2^{s+r}-2^{s-1}$ if $\beta > 1$

4. Multi–elementary attractors are also considered.

5. The sufficient condition for the iteration graph to be symmetric is that $\alpha=1$ or $\alpha=2$

6. The necessary and sufficient condition for the existence of the binary tree is that the modul should be a Fermat–prime.

7. An algorhitm is given which produces iteration graphs.

ÜBER EINE DISKRETE ITERATION DER ZAHLENTHEORIE

Die Arbeit behandelt eine spezielle diskrete Iteration, die jeder Restklasse mod M das Quadrat dieser Restklasse zuordnet, wobei M ein fixer Modul ist. Die Struktur des entstehenden Graphs der Iteration wird für verschiedene Moduln untersucht.

Die folgenden Bezeichnungen werden verwendet:
s – die Anzahl der verschiedenen Primteiler von M
r – die Anzahl der Primteiler der Form 6k+1 von M
t – die Anzahl der Primteiler nicht der Form 6k+1 von M
α – der Exponent von 2 in der Primzahlpotenzdarstellung von M
β – der Exponent von 3 in der Primzerlegung von M

Wir beweisen die folgenden Sätze.

1. Die Anzahl der Fixpunkte ist 2^s. Die Fixpunkte sind
   $x \equiv m_1^{\varphi(m_2)}$ mod M für alle m_1 und m_2, wobei
   $m_1 m_2 = M$ und $(m_1, m_2) = 1$ gelten.
2. Wenn $a^{\varphi(M)} \equiv t \bmod M$ gilt, dann ist t eine Lösung von $x^2 \equiv x \bmod M$ und wenn a läuft von 0 bis M–1, dann ist jede Lösung von $x^2 \equiv x \bmod M$ der Form $a^{\varphi(M)}$. (Das ist eine Verallgemeinerung des Eulerschen Satzes.)
3. Die Anzahl der zweielementigen Zyklen ist
   $2^{s+r-1} - 2^{s-1}$ für $\beta < 2$ bzw.
   $2^{s+r} - 2^{s-1}$ für $\beta > 1$.
4. $\alpha = 1$ oder $\alpha = 2$ ist eine hinreichende Bedingung für die Symmetrie des Graphes der Iteration.
5. Ein binärer Baum existiert dann und nur dann, wenn der Modul M eine Fermatsche Primzahl ist.

Außerdem untersuchen wir auch Attraktore und geben wir einen Algorithmus für die Darstellung des Graphes der Iteration.