MAN 060 – Elementär talteori
Sommaren 2007

Två faktoriseringsalgoritmer

Inte minst på grund av populariteten hos RSA-systemet för kryptering vars säkerhet är avhängig svårigheten att faktorisera stora tal, har de senaste decennierna stora ansträngningar gjorts att skapa nya algoritmer för detta problem. Vi visar här två sådana algoritmer, Pollard rho samt Pollard p – 1. Bägge lider av stora brister, men de är fullt användbara och framför allt intressanta tillämpningar på kongruensräkning.

Pollard rho

Pollard rho fungerar bäst när man vill faktorisera ett tal med en någorlunda liten primfaktor. Låt *m* vara talet som skall faktoriseras.
Bilda följden $\{x_n\}$ genom rekursionformeln $x_{n+1} = f(x_n)$, där *f* är ett polynom, till exempel $f(x) = x^2 + 1$ och x_0 något startvärde, till exempel $x_0 = 2$.
Bilda differenser $x_{2i} - x_i$, för $i = 1,2,3,\ldots$ och beräkna $(x_{2i} - x_i, m)$. Om denna största gemensamma delare är > 1 har vi naturligtvis en delare till *m*.

Idén med Pollard rho är att om *p* är litet – låt oss säga $< 10^{15}$ – är sannolikheten anständigt stor att $x_a \equiv x_b \pmod{p}$ för rimligt små tal *a* och *b*. Det finns skäl att tro att en sådan ”träff” inträffar efter sisådär $\sqrt{p}$ steg i rekursionen. I och med att en sådan kongruens uppstått blir följden $\{x_n\}$ periodisk och då kommer också $x_{2i} \equiv x_i \pmod{p}$ för något *i* där $(b-a)$ delar *i*. I så fall är $(x_{2i} - x_i, m) \geq p$ och vi har hittat en faktor till *m*.

Exempel:

Vi vill faktorisera talet 4469. Genom att välja $f(x) = x^2 + 1$ och $x_1 = 2$ bildas följden 2, 5, 26, 677, 2492, 2624, 3117, 84, 2588, 3183, 267, 4255, 1107, 944, och så vidare. Naturligtvis sker alla beräkningar modulo 4469

Successivt bildar vi differenser som ovan och beräknar största gemensamma delare med $m = 4469$

$(5-2,4469)=1$
$(677-5,4469)=1$
$(2624-26,4469)=1$
$(84-677,4469)=1$
$(3183-2492,4469)=1$
$(4255-2624,4469)=1$
$(944-3117,4469)=41$

En enkel division ger faktoriseringen $4469=41\cdot 109$

Pollard p – 1

Om *n*, det tal som skall faktoriseras, har en primfaktor *p* sådan att $p-1$ består av endast små primfaktorer, kan Pollard $p-1$ ge ett rimligt snabbt resultat.
I så fall finns nämligen ett inte alltför stort tal *k* sådant att $p-1$ delar $k!$, det vill säga så att $k!=c(p-1)$ för något heltal c.
Detta innebär att $2^{k!}=2^{c(p-1)}=\left(2^{p-1}\right)^c\equiv 1^c\equiv 1\pmod p$ eftersom $2^{p-1}\equiv 1\pmod p$. Alltså kommer *p* att dela $2^{k!}-1$ vilket gäller även om vi reducerar $2^{k!}$ modulo *n*. På samma sätt som i Pollard rho hittar vi *p* genom att beräkna $\left(2^{k!}-1,n\right)$ för $k=2,3,4,\ldots$
$2^{k!}$ blir snabbt ohanterligt stort men kan beräknas genom rekursionsföljden $r_k=r_{k-1}^k$ med $r_1=2$. Och givetvis reducerar man hela tiden modulo *n*.

Exempel:

Vi vill faktorisera talet 5371. Enligt ovan skall vi alltså beräkna $2^{k!}-1$ modulo 5371 vilket görs med hjälp av rekursionen $r_k=r_{k-1}^k$.
Vi erhåller följden 1, 3, 63, 3582, 1107 och så vidare.

För att hitta en primfaktor bildar vi successivt största gemensamma delare med 5371 och redan $(1107,5371)=41$, varpå vi lätt hittar faktoriseringen
$5371=41\cdot 131$

Notera att $41-1=40=2^3\cdot 5$ som delar 5!