MAN 060 – Elementär talteori
Sommaren 2007

Slantsingling

Som en oväntad och användbar tillämpning på kvadratisk reciprocitet skall vi här diskutera en lösning på problemet hur man på ett rättvist sätt singlar slant över elektronisk kommunikation.

Vi måste då först behandla kongruensen $x^2 \equiv a \pmod{n}$ där $n = pq$, p och q primtal.

Antag att vi vet att den givna kongruensen har en lösning x_0.
I så fall existerar lösningar även till $x^2 \equiv a \pmod{p}$ såväl som till $x^2 \equiv a \pmod{q}$.
Låt $x_1 \equiv x_0 \pmod{p}$ med $0 < x_1 < p$ och $x_2 \equiv x_0 \pmod{q}$ med $0 < x_2 < q$.
Då har $x^2 \equiv a \pmod{p}$ lösningarna $x \equiv \pm x_1 \pmod{p}$
och $x^2 \equiv a \pmod{q}$ lösningarna $x \equiv \pm x_2 \pmod{q}$.

Det finns fyra sätt att kombinera dessa lösningar på, och varje kombination ger enligt kinesiska restsatsen upphov till en unik lösning modulo *n*. Vi kan alltså hävda att talet *a* har fyra kvadratrötter modulo n.
Det är dessutom så att de fyra rötterna hänger ihop parvis.
Ty om systemet $\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv x_2 \pmod{q} \end{cases}$ har lösningen $x \equiv g \pmod{n}$
har systemet $\begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q} \end{cases}$ lösningen $x \equiv n - g \pmod{n}$.
På samma sätt om systemet $\begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv x_2 \pmod{q} \end{cases}$ har lösningen $x \equiv z \pmod{n}$
har systemet $\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q} \end{cases}$ lösningen $x \equiv n - z \pmod{n}$.

Om vi vidare förutsätter att $p \equiv q \equiv 3 \pmod{4}$ kan vi till och med explicit skriva upp
lösningarna till $x^2 \equiv a \pmod{p}$ respektive $x^2 \equiv a \pmod{q}$, nämligen $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$
respektive $x \equiv \pm a^{\frac{q+1}{4}} \pmod{q}$.
Detta eftersom $\left(a^{\frac{p+1}{4}} \right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \pmod{p}$ där den sista kongruensen gäller
eftersom $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p} \right) = 1 \pmod{p}$.
Och att *a* är en kvadratisk residy modulo *p* beror på att den är en kvadratisk residy modulo *n*, vilket vi förutsatte ovan.

Nu kan vi beskriva själva slantsinglingen. Vi tänker oss att Robert och Alice kommunicerar elektroniskt och måste fatta ett gemensamt beslut. De kan inte komma överens och litar inte på varandra och vill därför singla slant på ett sådant sätt att resultatet är acceptabelt för bägge.

Detta kan gå till på följande sätt:

Alice väljer två stora primtal *p* och *q*, sådana att $p \equiv q \equiv 3 \pmod 4$.
Hon skickar $n = pq$ till Robert.
Om Robert kan faktorisera *n* vinner han slantsinglingen.

Robert väljer ett godtyckligt heltal g, $g < n$ och skickar *a* med $a \equiv g^2 \pmod n$ till Alice.

Alice löser $a \equiv x^2 \pmod n$ enligt principen ovan och får alltså fyra lösningar som vi kan kalla $g, z, n-g, n-z$.
Hon väljer på måfå en av dessa fyra lösningar och skickar tillbaks den till Robert. Notera att Alice inte kan veta vilken av lösningarna som var Roberts ursprungliga val, alltså g.
Robert beräknar nu summan av sitt g och den lösning som Alice skickade och beräknar därefter största gemensamma delare till denna summa och *n*.
Följande gäller: $(g+z, n) = q$, $(g+n-z, n) = p$, $(g+g, n) = 1$, $(g+n-g, n) = n$.
Med andra ord har Robert en chans på två att med hjälp av den information som roten som Alice skickar innehåller faktorisera *n*.

Exempel: Alice väljer $p = 103, q = 107$ och skickar $n = 103 \cdot 107 = 11021$.
Robert väljer på måfå talet 212 som han kvadrerar och reducerar modulo *n*, $212^2 \equiv 860 \pmod n$. Så han skickar 860 till Alice.

Alice löser kongruensen $x^2 \equiv 860 \pmod n$ genom att först lösa
$x^2 \equiv 860 \equiv 36 \pmod{103}$ respektive $x^2 \equiv 860 \equiv 4 \pmod{107}$.

Lösningarna till $x^2 \equiv 36 \pmod{103}$ är $x \equiv 36^{\frac{103+1}{4}} \equiv \pm 36^{26} \equiv \pm 6 \pmod{103}$.

Lösningarna till $x^2 \equiv 4 \pmod{107}$ är $x \equiv 4^{\frac{107+1}{4}} \equiv \pm 4^{27} \equiv \pm 2 \pmod{107}$.

Hon kombinerar sedan dessa lösningar i fyra par och får med hjälp av kinesiska restsatsen de fyra lösningarna $g \equiv \pm 212$, $z \equiv \pm 109 \pmod n$.
Nu väljer Alice en av dessa lösningar och skickar den till Robert.
$g \equiv \pm 212$ hjälper inte Robert ett dyft, men skulle han händelsevis få $z \equiv \pm 109$ bildar han raskt summan med sitt ursprungliga val 212 och beräknar största gemensamma delare:
$(212 + 109, n) = (321, n) = 107$, eller $(212 - 109, n) = (103, n) = 103$.
Robert kan i detta senare fall faktorisera $n = 11021$ och vinner slantsinglingen.