



1 Inledning

Denna laboration syftar till att du skall få testa på att använda Maximas funktioner för talteori, skriva script, fördjupa dina kunskaper i talteori och få insikt i det viktigaste sättet att kryptera information.

Den talmängd vi skall räkna med i denna laboration är \mathbb{Z}_p där p är ett primtal. Exempelvis gäller att $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ och du skall tänka på \mathbb{Z}_5 som en "klocka" som börjar på 0 och där ett varv är 5. Då blir till exempel $2 + 4 = 1$, $2 \cdot 3 = 1$ och $1 - 3 = 3$.

Med detta sätt att räkna blir alltså talen -1, 4 och 19 i någon mening *samma* tal. Med ett finare språkbruk säger man att de är kongruenta modulo 5, vilket tecknas $-1 \equiv 4 \pmod{5}$. Vi gör följande definition.

Definition 1. Talen a och b är *kongruenta modulo m* om det går att skriva $a = b + z \cdot m$ för något heltal z . Detta tecknas $a \equiv b \pmod{m}$.

I exemplen ovan gäller ju att $4 = -1 + 1 \cdot 5$ och $4 = 19 - 3 \cdot 5$, men du bör nog ändå tänka dig att du räknar på en klocka.

Maximas funktion för att beräkna vad ett tal a blir modulo m heter $\text{mod}(a, m)$.

Denna laboration bygger helt på följande två satser.

Sats 2. *Ekvationen $ax + by = 1$ är bara lösbar i \mathbb{Z} om $\text{gcd}(a, b) = 1$. Mer allmänt gäller att ekvationen $ax + by = \text{gcd}(a, b)$ är lösbar i \mathbb{Z} .*

Sats 3. (Fermats lilla sats) *Om primtalet p och heltalet x är relativt prima, gäller $x^{p-1} \equiv 1 \pmod{p}$.*

Sats 2 känner du säkert igen från problem som brukar formuleras såhär: Antag att du har två hinkar, en som rymmer 13 liter och en som rymmer 5 liter, ett stort kärl och mycket vatten. Hur kan du bilda 1 liter vatten i kärlet. Detta problem kan formuleras $13x + 5y = 1$ och går alltså att lösa eftersom $\text{gcd}(13, 5) = 1$.

Maximas funktion för att lösa denna typ av ekvation heter $\text{gcdex}(a, b)$ där a och b har samma betydelse som ovan. Funktionen returnerar en lista som innehåller x , y och $\text{gcd}(a, b)$.

Sats 3 är lite märklig. Den uttalar sig egentligen om alla heltal, men i denna laboration är det mest relevant att tänka på en "klocka" där ett helt varv är ett primtal. I \mathbb{Z}_5 gäller alltså $1^4 = 1$, $2^4 = 1$, $3^4 = 1$ och $4^4 = 1$.

Att satsen kallas Fermats lilla sats beror på att den bevisades av Fermat (1601-1685) och det finns en mer berömd sats som Fermat också visade

som brukar kallas Fermats stora sats. (Den säger att ekvationen $a^n + b^n = c^n$ saknar lösningar i \mathbb{Z} om $n \in \mathbb{Z}, n > 2$)

Uppgift 4. Lös ekvationen $13x + 5y = 1$ själv (Huvudräkning!) och jämför Maxima.

Uppgift 5. Använd Maxima för att beräkna till exempel $7^4 \pmod{5}$, $21^{22} \pmod{23}$. Enligt sats 3 skall alltså resultatet bli 1 eftersom 5 och 23 är primtal.

2 RSA-kryptering

Sedan mycket lång tid har man haft behov av att hålla information hemlig. För att kunna meddela någon på annan plats något hemligt måste man uppfinna ett sätt att kryptera informationen. Romarna använde till exempel ett mycket enkelt krypto som gick ut på att byta A mot till exempel S, B mot T, C mot U och så vidare till Ö mot R. Detta är inte ett speciellt bra krypto, eftersom det är så lätt att knäcka det för någon som har kommit över den krypterade informationen.

Ett problem med den typ av krypto som beskrevs ovan är att mottagare och sändare av informationen måste komma överens om nyckeln i förväg. Med nyckel menas här det som gör det möjligt att kryptera eller dekryptera informationen. År 1978 publicerade tre herrar vid namn Rivest, Shamir och Adleman en metod att kryptera och dekryptera som går ut på att man använder sig av en så kallad *öppen nyckel*. Metoden benämns idag RSA-kryptering.

Som ett exempel på ett sätt att använda metoden kan vi ta en skola, där eleverna vill skicka hemliga meddelanden till varandra. Det finns en anslagstavla där alla som vill kunna ta emot ett hemligt meddelande skriver ned två tal (hur de konstrueras går vi igenom nedan), och det finns ett postfack.

Antag att Alice vill skicka ett meddelande till Bob (i litteratur om kryptering i engelska texter heter alltid personerna Alice och Bob, istället för A och B). Hon går då till anslagstavlan och kollar vilka tal Bob har skrivit upp. Dessa använder hon för att kryptera sitt meddelande, som hon sedan lägger i postfacket. Meddelandet kan ligga i det allmänna postfacket eftersom ingen annan än Bob kan dekryptera det, eftersom bara Bob själv vet hur de två talen han skrivit upp har bildats.

Om Bob vill svara Alice måste han gå till anslagstavlan och kolla vilka tal hon har skrivit upp, och använda dessa. Poängen är hur som helst att alla nycklar är öppna, alla som vill kan titta på anslagstavlan.

3 Metoden i detalj

Vi skall nu i detalj gå igenom hur RSA-kryptering fungerar. Den bygger helt på de två satserna ovan. Du skall själv konstruera nyckeln och till slut skall någon annan kunna skicka meddelanden till dig, som bara du skall kunna läsa. Uppgifterna nedan löser du i ett Maxima-script.

Uppgift 6. Välj två primtal, p och q .

Uppgift 7. Bilda talen $m = (p - 1)(q - 1)$ och $n = pq$.

Uppgift 8. Nu skall du hitta två tal d och e så att $d \cdot e \equiv 1 \pmod{m}$.

Det kanske inte är helt uppenbart hur man hittar ett sådant par, men såhär kan man resonera. Enligt definition 1 betyder det att det skall finnas ett tal z så att

$$d \cdot e = 1 + z \cdot m.$$

Om denna ekvation skriv som till

$$d \cdot e - z \cdot m = 1$$

ser du att sats 2 säger att denna ekvation bara kan ha en lösning om till exempel d och m är relativt prima. Välj därför först ett tal d som uppfyller detta villkor, och lös sedan ekvationen så att du får ett värde på e . (Värdet på z kommer du inte att behöva använda.)

Nu har du ett par av tal (d, n) som du kan publicera som en öppen nyckel som vem som helst kan använda för att kryptera meddelanden till dig. Detsamma gäller naturligtvis dina kurskamrater. Det är viktigt att du håller talet e hemligt!

Uppgift 9. Tag emot en nyckel från någon annan. Bestäm dig för ett meddelande som du vill skicka. Av praktiska skäl kan det inte vara för långt, i själva verket bara ett enda tecken till att börja med. Låt bokstaven A stå för 1, B för 2 och så vidare. Omvandla på detta sätt ditt tecken till ett tal x .

Uppgift 10. Beräkna $y = x^d \pmod{n}$. Här skall du alltså inte använda din egen nyckel, utan den du fick från den du vill skicka ditt tecken till. Meddela mottagaren talet y .

För att du skall lära dig dekryptera meddelanden måste du nu ta emot ett annat tal y från någon annan, som har bildat detta tal med din nyckel.

Uppgift 11. Dekryptera det mottagna meddelande y genom att beräkna $x = y^e \pmod{n}$. Nu skall du alltså använda ditt tal e .

4 Varför fungerar metoden?

Poängen sammanfattas i följande sats.

Sats 12.

$$x^{de} \equiv x \pmod{n}$$

Utskriven i flera steg ser du att meddelandet x som skickades till dig först krypterades till y med $y = x^d$. Sedan beräknade du $y^e = (x^d)^e = x^{de}$ och då säger alltså satsen att detta är lika med det ursprungliga talet x .

Bevis. Det som skall visas är att

$$x^{de} \equiv x \pmod{n}.$$

Det kan lika gärna skrivas som

$$x^{de} - x \equiv 0 \pmod{n},$$

vilket betyder att n måste dela differensen $x^{de} - x$. Nu är ju n bildat genom $n = pq$ så det räcker att visa att p och q delar $x^{de} - x$ var för sig.

Eftersom $de \equiv 1 \pmod{m}$ gäller enligt definition 1 att $de = 1 + km$. Talet m definierades som $m = (p-1)(q-1)$, därmed gäller då $de = 1 + k(p-1)(q-1)$. Vi har nu att

$$x^{de} = x^{1+k(p-1)(q-1)} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{p-1})^{k(q-1)} \equiv x \cdot 1^{k(q-1)} \pmod{p}.$$

I det sista steget har sats 3 använts. Naturligtvis gäller $1^{k(q-1)} = 1$, så högerledet ovan är helt enkelt lika med talet x .

På precis samma sätt argumenterar man för att $x^{de} \equiv x \pmod{q}$. Därmed gäller $x^{de} \equiv x \pmod{n}$. \square

Uppgift 13. Varför räcker det med att visa att p och q delar differensen var för sig?

Uppgift 14. (Frivillig) Lär dig så mycket du vill om modulär aritmetik (eng modular arithmetic) från till exempel Wikipedia.