Avsnitt 2

Tillägg om kongruensräkning

Sats 2.1 (Kinesiska restsatsen) *Låt n och m vara relativt prima heltal samt a och b två godtyckliga heltal. Då har ekvationssystemet*

$$\begin{cases} x & \equiv & a \bmod n \\ x & \equiv & b \bmod m \end{cases}$$

en lösning. Om c är en lösning, ges samtliga lösningar av $x = c + knm$, där k är ett godtyckligt heltal.

Eftersom vi kan välja k godtyckligt och alla lösningar är av formen $c + knm$ finns det precis en lösning som ligger mellan 0 och $nm - 1$. Det finns alltså precis en rest vid division med nm som löser ekvationssystemet (under förutsättning att n och m är relativt prima förstås).

Kinesiska restsatsen säger alltså, bland annat, att om vi har rester a och b vid division med n respektive m, så finns det en entydig (d.v.s precis en) rest c vid division med nm, så att $c \equiv a \bmod n$ och $c \equiv b \bmod m$.

Bevis. Eftersom n och m är relativt prima har vi att $\mathrm{SGD}(n, m) = 1 = yn + zm$, för några heltal y och z. Vi har då $1 \equiv zm \bmod n$ och $1 \equiv yn \bmod m$. Sätter vi nu $c = byn + azm$ har vi $c \equiv azm \equiv a \cdot 1 \equiv a \bmod n$ och $c \equiv byn \equiv b \cdot 1 \equiv b \bmod m$. Detta visar att c löser ekvationssystemet.

Antag nu att även c' löser ekvationssystemet. Vi har då att $c' - c \equiv a - a \equiv 0 \bmod n$, så $c' - c = ln$, för något heltal l. På samma sätt har vi att $m \mid c' - c$, d.v.s att $m \mid nl$. Men m och n är relativt prima och därför måste m dela l, d.v.s

$l = km$, och $c' - c = kmn$, för något heltal k. Detta visar att $c' = c + kmn$, för något heltal k.

Å andra sidan har vi att alla tal av formen $c + kmn$ löser ekvationssystemet, eftersom $c + kmn \equiv c \equiv a \bmod n$ och $c + kmn \equiv c \equiv b \bmod m$. ■

Beviset ger en metod för att lösa ekvationssystemet. Vi illusterar denna med

Exempel 2.1 Lös ekvationssystemet

$$\begin{cases} x & \equiv & 23 \bmod 31 \\ x & \equiv & 24 \bmod 32 \end{cases}$$

Observera att 31 och 32 är relativt prima så vi vet säkert att ekvationssystemet har lösningar (i själva verket oändligt många). Vi har $1 = 32 - 31$. Sätter vi $x = 23 \cdot 32 - 24 \cdot 31$ har vi $x \equiv 23 \bmod 31$ och $x \equiv -24(-1) \equiv 24 \bmod 32$. Samtliga lösningar ges av $x = 23 \cdot 32 - 24 \cdot 31 + 31 \cdot 32k = -8 + 992k$, där k är ett godtyckligt heltal.

Detta är alltså den metod som anvädns i beviset och som lämpar sig för teoretiska resonemang. I praktiken är det dock lättare att lösa ekvationenssystemet geonom att successivt lösa ekvationerna (nerifrån t.ex.):

Den andra ekvationen ger att $x = 24 + 32k_1$, där k_1 är ett godtyckligt heltal. Insättning i den första ekvationen ger sedan att $24 + 32k_1 \equiv 23 \bmod 31$, eller $k_1 \equiv -1 \bmod 31$, så vi ska ha att $k_1 = -1 + k_2 31$, där k_2 är ett godtyckligt heltal.

Sätter vi in detta i $x = 24 + 32k_1$, får vi att $x = 24 + 32(-1 + k_2 31) = -8 + 992k_2$, där k_2 är ett godtyckligt heltal, löser båda ekvationerna i systemet.

Man bör observera att Kinesiska restsatsen *inte* gäller om förutsättningen att n och m ska vara relativt prima stryks.

Exempel 2.2 Ekvationssystemet

$$\begin{cases} x & \equiv & 1 \bmod 4 \\ x & \equiv & 2 \bmod 6 \end{cases}$$

saknar lösning. Den andra ekvationen ger att $x = 2 + 6k$, för något k. Insättning i den första ger $1 \equiv 2 + 2k$ och, efter multiplikation med 2, $2 \equiv 0 \bmod 4$, vilket är absurt.

Kinesiska restsatsen är användbar för att förenkla när man vill lösa problem modulo tal som inte är potenser av ett primtal:

Exempel 2.3 För vilka heltal y gäller att $15 \mid y^2 + 3y + 2$?

Eftersom $15 = 3 \cdot 5$ och 3 och 5 är relativt prima gäller att $15 \mid a$ om och endast om $3 \mid a$ och $5 \mid a$. Vi undersöker för vilka y som 3 respektive 5 delar uttrycket genom att räkna modulo 3 respektive 5.

Insättning av 0, 1, 2 ger att $0 \equiv y^2 + 3y + 2 \equiv y^2 + 2 \bmod 3$ har lösningarna $y \equiv 1 \bmod 3$ och $y \equiv 2 \bmod 3$. Räkningarna modulo 5 är lite besvärligare, så vi gör en tabell

y	$3y$	y^2	$y^2 + 3y + 2$
0	0	0	2
1	3	1	1
2	1	4	2
3	4	4	0
4	2	1	0

Vi ser att vi måste ha $y \equiv 3 \bmod 5$ eller $y \equiv 4 \bmod 5$. Vi ska nu lösa de fyra ekvationssystemen

$$\begin{cases} y \equiv 1 \bmod 3 \\ y \equiv 3 \bmod 5 \end{cases} \quad \begin{cases} y \equiv 2 \bmod 3 \\ y \equiv 3 \bmod 5 \end{cases} \quad \begin{cases} y \equiv 1 \bmod 3 \\ y \equiv 4 \bmod 5 \end{cases} \quad \begin{cases} y \equiv 2 \bmod 3 \\ y \equiv 4 \bmod 5 \end{cases}$$

Lösningarna är, i tur och ordning, $y = 13 + 15k$, $8 + 15k$, $4 + 15k$, $14 + 15k$, där k är ett godtyckligt heltal. Vi har alltså att $15 \mid y^2 + 3y + 2$ om och endast om y är kongruent 4, 8, 13 eller 14 modulo 15.

Kinesiska restsatsen kan lätt generaliseras:

Sats 2.2 *Antag att talen $n_1, n_2, \ldots, n_i$ är parvis relativt prima heltal och att heltalen $a_1, a_2, \ldots, a_i$ är givna. Då har ekvationssystemet*

$$\begin{cases} x = a_1 \bmod n_1 \\ x = a_2 \bmod n_2 \\ \quad \vdots \\ x = a_i \bmod n_i. \end{cases}$$

en lösning. Om c är en lösning, ges samtliga lösningar av $x = c + k(n_1 n_2 \ldots n_i)$, där k är ett godtyckligt heltal.

Exempel 2.4 För vilka heltal x gäller att

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 7 \end{cases}$$

Vi ska gå tillväga på följande vis. Först bestämmer vi alla lösningar till den nedersta ekvationen. Vi avgör sedan vilka av dessa som löser den andra ekvationen. Tillsist ska vi avgöra vilka av lösningarna till de två nedersta ekvationerna som även löser den första.

Den nedersta ekvationen har lösningarna $x = 4+k_1 7$, där k_1 är ett godtyckligt heltal.

Vi bestämmer nu k_1 så att $x = 4 + 7k_1$ även löser den andra ekvationen genom insättning. Vi får

$$4 + k_1 7 \equiv 3 \bmod 5 \Leftrightarrow 2k_1 \equiv -1 \equiv 4 \bmod 5.$$

Multiplikation med 3 ger nu $k_1 \equiv 12 \equiv 2$, eller att $k_1 = 2 + k_2 5$, där k_2 är ett godtyckligt heltal. Detta ger

$$x = 4 + 7k_1 = 4 + 7(2 + 5k_2) = 18 + 35k_2.$$

De heltal som löser de båda nedersta ekvationerna är alltså de som har formen $18 + 35k_2$, där k_2 är ett godtyckligt heltal.

Vi bestämmer nu k_2 så att $x = 18 + 35k_2$ även löser den första ekvationen genom insättning. Vi får

$$18 + 35k_2 \equiv 1 \bmod 2 \Leftrightarrow k_2 \equiv 1 \bmod 2 \Leftrightarrow k_2 = 1 + 2k_3,$$

där k_3 är ett godtyckligt heltal. Detta ger nu att

$$x = 18 + 35k_2 = 53 + 70k_3.$$

Samtliga lösningar ges av $x = 53 + 70k$, där k är ett godtyckligt heltal.

I det sista exemplet löste vi $2k \equiv 4 \bmod 5$ genom att multiplicera de båda leden med 3. Anledningen var naturligt vis att $3 \cdot 2 \equiv 1 \bmod 5$. Talet 3 är alltså en *invers* till 2 modulo 5.

Definition 2.1 Talet a är en *invers* till b modulo n om $ab \equiv 1 \bmod n$.

Det är inte säkert att ett tal *har* en invers modulo n. T.ex. saknar 4 invers modulo 6. Om nämligen a vore inversen skulle vi ha $a4 \equiv 1 \bmod 6$ och multiplikation med 3 skulle ge absurditeten $0 \equiv 3 \bmod 6$. Följande sats klargör precis när en invers existerar

Sats 2.3 *Talet b är inverterbart modulo n om och endast om $SGD(b, n) = 1$.*

Bevis. Om b är inverterbart finns a så att $ab \equiv 1 \bmod n$, d.v.s $ab = 1+kn$ för något heltal k. Räkning modulo $\mathrm{SGD}(b,n)$ ger $0 \equiv 1 \bmod \mathrm{SGD}(b,n)$, d.v.s $\mathrm{SGD}(b,n) \mid 1$, så $\mathrm{SGD}(b,n) = 1$.

Antag å andra sidan att $\mathrm{SGD}(b,n) = 1$. Då finns tal a och k så att $1 = ab+kn$. Räkning modulo n ger $1 \equiv ab \bmod n$, d.v.s b är inverterbart modulo n. ■

Beviset ger en metod för att avgöra om det går att invertera b och i så fall bestämma a: Beräkna $\mathrm{SGD}(b,n)$ med Euklides algoritm, om $\mathrm{SGD}(b,n) = 1$ är b inverterbart annars inte. Bestäm a och k så att $ab+kn = 1$ med Euklides algoritm baklänges, om $\mathrm{SGD}(b,n) = 1$.

Använder vi detta på 2 modulo 5 får vi $5 = 2 \cdot 2 + 1$, $1 = -2 \cdot 2 + 5$, d.v.s $1 \equiv 3 \cdot 2 \bmod 5$.

Exempel 2.5 Avgör om 37 är intverterbart modulo 91 och bestäm i så fall dess invers.

Euklides algoritm ger

$$\begin{aligned} 91 &= 2 \cdot 37 + 17 \\ 37 &= 2 \cdot 17 + 3 \\ 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Alltså är $\mathrm{SGD}(37, 91) = 1$ och 37 är inverterbart modulo 91.

För att bestämma inversen till 37 gör vi Euklides algoritm baklänges och får

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (17 - 5 \cdot 3) = 6 \cdot 3 - 1 \cdot 17 = 6 \cdot (37 - 2 \cdot 17) - 1 \cdot 17 = \\ &= 6 \cdot 37 - 13 \cdot 17 = 6 \cdot 37 - 13(91 - 2 \cdot 37) = 32 \cdot 37 - 13 \cdot 91. \end{aligned}$$

Räknar vi nu modulo 91 ser vi att $1 \equiv 32 \cdot 37 \bmod 91$, så 32 är en invers till 37 modulo 91.

Exempel 2.6 Den sluge gamle kinesiske generalen Huang hade ett finurligt sätt att räkna sina mannar efter strid. Före striden hade han 4711 soldater. Efter striden lät han dem ställa upp på 13 jämna led och lät anteckna hur många som blev över. Han lät sedan ställa upp dem i 17 och 23 jämna led. Antalet soldater som blev över var, i tur och ordning, 3, 12 och 2. Hur många soldater hade general Huang kvar?

Ekvationssytemet

$$\begin{cases} x \equiv 3 \mod 13 \\ x \equiv 12 \mod 17 \\ x \equiv 2 \mod 23 \end{cases}$$

har precis en lösning mindre än $13 \cdot 17 \cdot 23 = 5083$, ty talen 13, 17, och 23 är parvis relativt prima. Sista ekvationen ger $x = 2 + 23k_1$ som insatt i den andra ger $2 + 6k_1 \equiv 12 \mod 17$, d.v.s $6k_1 \equiv 10 \mod 17$. Multiplikation med 3, som är invers till 6 modulo 17, ger $k_2 \equiv 13 \mod 17$, eller $k_1 = 13 + 17k_2$. Därmed har vi $x = 2 + 23k_1 = 2 + 23(13 + 17k_2) = 301 + 391k_2$. Insatt i första ekvationen ger detta $2 + k_2 \equiv 3 \mod 13$, d.v.s $k_2 \equiv 1 \mod 13$, så $k_2 = 1 + 13k_3$ och $x = 301 + 391k_2 = 301 + 391(1 + 13k_3) = 692 + 5083k_3$. Generalen hade alltså 692 soldater kvar.

Sats 2.4 (Fermats lilla sats) *Om p är ett primtal, så gäller för varje heltal a att $a^p \equiv a \mod p$.*

Bevis. Om p delar a är båda sidor av likheten 0, så vi kan utgå från att a och p är reltivt prima, eftersom p är ett primtal. Där med är a inverterbart modulo p. Låt b vara en invers till a modulo p så att $ab \equiv 1 \mod p$.

När talen 1, 2, 3, ..., $p-1$ multipliceras med a får vi talen $1 \cdot a$, $2 \cdot a$, $3 \cdot a$, ..., $(p-1)a$, som alla har olika rester modulo p eftersom a är inverterbart modulo p. Den nya listans rester vid division med p är alltså någon uppräkning av sammma tal som i den första. Tar vi därför produkterna av talen i de båda listorna var för sig får vi

$$(p-1)! \equiv (p-1)!a^{p-1} \mod p$$

Eftersom $(p-1)!$ inte är delbart med primtalet p är det inverterbart modulo p. Multiplikation med en invers modulo p till detta tal ger därför

$$1 \equiv a^{p-1} \mod p.$$

Multiplikation med a ger till sist

$$a \equiv a^p \mod p.$$

■

Av Fermats lilla sats följer att $a^{p^k} \equiv a \bmod p$, när p är ett primtal:

$$a^p \equiv a \Rightarrow (a^p)^p \equiv a^p \Rightarrow a^{p^2} \equiv a$$

$$a^{p^2} \equiv a \Rightarrow (a^{p^2})^p \equiv a^p \Rightarrow a^{p^3} \equiv a \text{ etc.}$$

Exempel 2.7 Visa att $66 \mid n^{11} - n$, för varje heltal n.
Eftersom $66 = 2 \cdot 3 \cdot 11$ och 2, 3 samt 11 är olika primtal räcker det att visa att $n^{11} - n \equiv 0$ i mdoulo 2, 3 och 11.

Vi använder Fermats lilla sats och räknar först modulo 2, så att $n^{2^k} = n$. Eftersom $11 = 2^3 + 2 + 1$ har vi

$$n^{11} \equiv n^{2^3} n^2 n^1 \equiv nnn \equiv n^3 \equiv n^2 n^1 \equiv nn \equiv n^2 \equiv n.$$

Vi räknar modulo 3 och har då $n^{3^k} \equiv n$:

$$n^{11} \equiv n^{3^2} n^2 \equiv nn^2 \equiv n^3 \equiv n.$$

Modulo 11 ger Fermats lilla sats direkt att $n^{11} \equiv n$.

2.1 Övningar

Övning 2.1 Undersök om b är inverterbart modulo n och bestäm en invers i förekommande fall, om

a) $b = 3$ och $n = 11$ b) $b = 7$ och $n = 25$ c) $b = 39$ och $n = 65$ d) $b = 93$ och $n = 101$.

Övning 2.2 Lös ekvationssystemet

a) $\begin{cases} x \equiv 12 \mod 49 \\ x \equiv 7 \mod 53 \end{cases}$ b) $\begin{cases} x \equiv 12 \mod 31 \\ x \equiv 7 \mod 43 \end{cases}$ c) $\begin{cases} x \equiv 5 \mod 13 \\ x \equiv 7 \mod 15. \end{cases}$

Övning 2.3 Lös ekvationssystemet

a) $\begin{cases} x \equiv 32 \mod 63 \\ x \equiv 33 \mod 64 \\ x \equiv 34 \mod 65 \end{cases}$ b) $\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 11 \\ x \equiv 2 \mod 14 \end{cases}$ c) $\begin{cases} x \equiv 6 \mod 7 \\ x \equiv 3 \mod 11 \\ x \equiv 5 \mod 15. \end{cases}$

Övning 2.4 Bestäm alla positiva heltal mindre än eller lika med 1984, sådana att resterna vid division med 3, 23 och 29 blir 2, 3 respektive 4.

Övning 2.5 Ett antal enkronor ska räknas. Man vet att om de fördelas jämt på 3 staplar blir det 2 över. Fördelas de lika på 14 respektive 23 staplar blir det 13 respektive 3 över. Antalet enkronor är mindre än 1000 stycken. Hur många är de?

Övning 2.6 Bestäm alla naturliga tal n sådana att
a) $2n^2 + 4n + 5$ är delbart med 105 b) $n^3 + 2n - 3$ är delbart med 63
c) $n^4 + n^3 + 2n + 1$ är delbart med 30 d) $n^2 + 3n + 4$ är delbart med 210.

Övning 2.7 Antalet tal mellan 0 och $n - 1$ (d.v.s antalet rester vid division med n), som är inverterbara modulo n betecknas $\phi(n)$. Funktionen ϕ kallas *Eulers ϕ-funktion*.
a) Vilka heltal mellan 0 och 13 är inverterbara modulo 14?
b) Antag att n och m är relativt prima. Visa att a är inverterbart modulo nm om och endast om det är inverterbart modulo n och m.
c) Vad är $\phi(14)$?

Övning 2.8 Visa att

a) $798 \mid n^{19} - n$ b) $546 \mid n^{13} - n$ c) $870 \mid n^{29} - n$,

för varje heltal n.

Övning 2.9 Visa att om p är ett primtal $\neq 2, 5$, så gäller att p delar $\underbrace{99\ldots9}_{p-1}$. Vad är $\underbrace{99\ldots9}_{p-1}$ modulo 2 och 5?

Övning 2.10 Bestäm slutsiffran i

a) 2^{110011} b) 47^{675} c) 1333^{19876}.

2.2 Förslag till svar

2.1 a) t.ex. 4 b) t.ex. 18 c) ej inverterbart d) t.ex. 63.

2.2 a) $2021+2597k$ b) $136+1333k$ c) $187+195k$, där k är ett godtyckligt heltal.

2.3 a) $x = -31 + k65 \cdot 64 \cdot 63$ b) $478 + 770k$ c) $-85 + 1155k$, där k är ett godtyckligt heltal.

2.4 1889

2.5 923

2.6 a) $23{+}105\text{k}, 38{+}105\text{k}, 65{+}105\text{k}, 80{+}105\text{k}$ b) $1{+}63\text{k}, 15{+}63\text{k}, 29{+}63\text{k}$, där k är ett godtyckligt heltal c) lösning saknas d) lösning saknas.

2.7 c) $\phi(14) = 6$.

2.8 Faktorisera 546, 798 samt 870 och använd Fermats lilla sats.

2.9 Observera att $99\ldots9 = 10^{p-1} - 1$. $99\ldots9 = -1$ modulo 2 och 5.

2.10 a) 8 b) 3 c) 1.