Homework 1

Elliot Duchek

Maj 2023

1 Fråga 1

(a)

$$1619x + 460y = 100 \tag{1}$$

H.L. 100 måste vara delbart med $SGD(1619, 460)$ eftersom vänsterledet per definition är det. Börja med att hitta $SGD(1619, 460)$ med Euklides algoritm.

$$\begin{aligned} 1619 &= 3(460) + 239 \\ 460 &= 1(239) + 221 \\ 239 &= 1(221) + 18 \\ 221 &= 12(18) + 5 \\ 18 &= 3(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \\ 2 &= 2(1) + 0 \end{aligned} \tag{2}$$

Ekvation 2 ger att $SGD(1619, 460) = 1$, vilket innebär att ekvation 1 har lösningar för godtyckligt heltal i H.L. Euklides algoritm baklänges ger

$$\begin{aligned} 1 &= 3 - 1(2) \\ &= 3 - 1(5 - 1(3)) = 2(3) - 1(5) \\ &= 2(18 - 3(5)) - 1(5) = 2(18) - 7(5) \\ &= 2(18) - 7(221 - 12(18)) = 86(18) - 7(221) \\ &= 86(239 - 1(221)) - 7(221) = 86(239) - 93(221) \\ &= 86(239) - 93(460 - 1(239)) = 179(239) - 93(460) \\ &= 179(1619 - 3(460)) - 93(460) = 179(1619) - 630(460). \end{aligned} \tag{3}$$

Ekvation 3 ger att

$$\begin{aligned} 1 &= 179(1619) - 630(460) \\ \implies 100 &= 17900(1619) - 63000(460). \end{aligned}$$

Alltså är $x = 17900$, $y = -63000$ en lösning till ekvation 1. Den allmänna lösningen ges av formeln

$$\begin{cases} x = mx_0 - \frac{b}{d}n \\ y = my_0 + \frac{a}{d}n \end{cases}$$

, där $m = 100$, $x_0 = 179, y_0 = -630, a = 1619, b = 460, d = 1$ och $n \in \mathbb{Z}$ är en valfri parameter. Slutligen har vi alltså

$$\begin{cases} x = 17900 - 460n \\ y = -63000 + 1619n \end{cases} \quad n \in \mathbb{Z}$$

(b)

$$\begin{cases} x = 17900 - 460n \\ y = -63000 + 1619n \end{cases}$$

Beloppet av x och y ger 4 fall.

Fall 1: $x \geq 0$, $y \geq 0$ Vi har då

$$\begin{cases} |x| = x = 17900 - 460n \\ |y| = y = -63000 + 1619n \end{cases}.$$

Detta ger

$$\begin{aligned} |x| + |y| &= 17900 - 460n - 63000 + 1619n \\ &= -45100 + 1159n \end{aligned} \tag{4}$$

Fall 2: $x < 0$, $y < 0$

$$\begin{cases} |x| = -x = -17900 + 460n \\ |y| = -y = 63000 - 1619n \end{cases}.$$

$$\begin{aligned} |x| + |y| &= -17900 + 460n + 63000 - 1619n \\ &= 45100 - 1159n \end{aligned} \tag{5}$$

Fall 3: $x < 0$, $y \geq 0$

$$\begin{cases} |x| = -x = -17900 + 460n \\ |y| = y = -63000 + 1619n \end{cases}.$$

$$\begin{aligned} |x| + |y| &= -17900 + 460n - 63000 + 1619n \\ &= -80900 + 2079n \end{aligned} \tag{6}$$

Fall 4: $x \geq 0$, $y < 0$

$$\begin{cases} |x| = x = 17900 - 460n \\ |y| = -y = 63000 - 1619n \end{cases}.$$

$$\begin{aligned} |x| + |y| &= 17900 - 460n + 63000 - 1619n \\ &= 80900 - 2079n \end{aligned} \tag{7}$$

Sätter vi ekvationerna 4, 5, 6 och 7 lika med 0 ser vi att ekvation 4 och 5 är ekvivalenta, och detsamma gäller 6 och 7. Alltså räcker det om vi endast betraktar ekvation 5 och 7. Lösningen som minimerar $|x|+|y|$ i fall 2 är

$$\begin{aligned} & 0 = 45100 - 1159n \\ \implies & n = \frac{45100}{1159} \approx 38.91 \approx 39 \\ \implies & x = -40,\ y = 101. \end{aligned} \tag{8}$$

Men detta är en falsk lösning i denna kontext då vi i fall 2 antog att både x och y var mindre än noll, men denna lösning ger att $y > 0$. Det som minimerar ekvationen i fall 4 ges av

$$\begin{aligned} & 0 = 80900 - 2079n \\ \implies & n = \frac{80900}{2079} \approx 38.91 \approx 39 \\ \implies & x = -40,\ y = 101. \end{aligned} \tag{9}$$

Vi får alltså $n = 39$ igen, vilket är ogiltigt även i denna kontext. Jag kan inte förklara varför metoden jag använder (falluppdelning) inte ger rätt lösning, men det är uppenbart att den inte gör det.

(c) Betrakta $4857x \equiv b \pmod{1380}$. Vi har att

$$\begin{aligned} & 4857x \equiv b \pmod{1380} \\ \iff & 4857x - b \equiv 0 \\ \iff & 1380 | 4857x - b \\ \iff & \exists\, a \in \mathbb{Z} : 4857x - b = 1380a \\ \iff & 4857x - 1380a = b. \end{aligned}$$

Alltså har kongruensen $4857x \equiv b \pmod{1380}$ lösningar omm den Diofantiska ekvationen $4857x - 1380a = b$ har lösningar, vilket bara inträffar då $d|b$, $d = SGD(4857, 1380)$ (ty d delar H.L., alltså måste d även dela V.L.). Eftersom siffersummorna av 4857 och 1380 båda är delbara med 3 är även

talen delbara med 3. $\frac{4857}{3} = 1619$ och $\frac{1380}{3} = 460$. I uppgift 1 (a) visade det sig att 1619 och 460 är relativt prima, alltså är $SGD(4857, 1380) = 3$, och kongruensen har alltså enbart lösningar då $3|b$.

Om $b = 12$ har vi $4857x \equiv 12 \pmod{1380}$, vilket svarar mot den Diofantiska ekvationen

$$4857x - 1380a = 12$$

för något $a \in \mathbb{Z}$. Delar vi bådar sidor med 3 får vi

$$1619x - 460a = 4$$

vilket svarar mot kongruensen

$$1619x \equiv 4 \pmod{460}.$$

Eftersom $SGD(1619, 460) = 1$ har 1619 invers i $\mathbb{Z}_{460}$. Låter vi $c = 1619^{-1}$ söker vi alltså lösningen till

$$1619c \equiv 1 \pmod{460}.$$

Kongruensen är ekvivalent med den Diofantiska ekvationen

$$1619c - 460a = 1.$$

En lösning till denna kan fås genom Euklides algoritm. Enligt ekvation 3 är en lösning

$$1619(179) - 460(630) = 1.$$

Alltså är $c \equiv 1619^{-1} \equiv 179 \pmod{460}$. Detta ger att

$$\begin{aligned} & 4857x \equiv 12 \pmod{460} \\ \iff & 1619x \equiv 4 \pmod{460} \\ \iff & x \equiv 4 \cdot 179 \pmod{460}. \end{aligned}$$

Slutligen har vi alltså

$$x \equiv (716 + n460) \pmod{460},\ n \in \mathbb{Z}.$$

Det följer att den minsta positiva heltalslösningen är

$$x \equiv 256 \pmod{460}.$$

(d) Eftersom $SGD(1619, 460) = 1$ (enl. ekvation 2) är $1619^{\Phi(460)} \equiv 1 \pmod{460}$ enligt Eulers sats. $\Phi(460)$ kan beräknas genom att primtalsfaktorisera 460. Gör vi detta ser vi att $460 = 2^2 \cdot 5 \cdot 23$. Alltså är

$$\Phi(460) = \Phi(2^2)\Phi(5)\Phi(23) = (2^2 - 2^0)(5^1 - 5^0)(23^1 - 23^0) = 176.$$

Notera att $351 = 352 - 1 = 2 \cdot 176 - 1$. Vi har alltså, enigt Eulers sats

$$\begin{aligned} 1619^{351} &\equiv \left(1619^{176}\right)^2 \cdot 1619^{-1} \pmod{460} \\ &\equiv 1^2 \cdot 1619^{-1} \\ &\equiv 1619^{-1}. \end{aligned}$$

Denna invers beräknades i föregående uppgift (c), och vi har att $1619^{-1} \equiv 179 \pmod{460}$. Slutligen har vi alltså

$$1619^{351} \equiv 1619^{-1} \equiv 179 \pmod{460}.$$

(e) För att använda upprepad kvadrering måste vi först skriva om basen 1619 i binär form. Detta görs genom att upprepade gånger dividera 1619 med 2 och notera resten vid varje division. Detta upprepas tills man når steget att dela 0 med 2, då är algoritmen klar. Man delar alltså inte 0 med 2, utan skriver ner resterna från tidigare divisioner så att resten från den första divisionen (351/2) hamnar längst till höger i det binära talet. Denna följd av 1:or och 0:or är talet på binär form. Vi får alltså

$$\begin{aligned} &(351)_2 = 101011111 \\ \iff\ &351 = 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 \end{aligned}$$

Nu behöver vi beräkna $x_0, x_1, \ldots, x_8$ där

$$\begin{aligned} x_0 &\equiv 1619 \pmod{460} \\ x_{i+1} &\equiv x_i^2 \equiv 1619^{2^i} \pmod{460}. \end{aligned}$$

Vi har

$$\begin{aligned} x_0 &\equiv 1619 \equiv 239 \pmod{460} \\ x_1 &\equiv 239^2 \equiv 81 \\ x_2 &\equiv 81^2 \equiv 121 \\ x_3 &\equiv 121^2 \equiv 381 \\ x_4 &\equiv 381^2 \equiv 261 \\ x_5 &\equiv 261^2 \equiv 41 \\ x_6 &\equiv 41^2 \equiv 301 \\ x_7 &\equiv 301^2 \equiv 441 \\ x_8 &\equiv 441^2 \equiv 361 \end{aligned} \tag{10}$$

Eftersom vi tidigare skrev om 351 i bas 2 vet vi att vi kan skriva

$$\begin{aligned} 1619^{351} &\equiv 1619^{2^8+2^6+2^4+2^3+2^2+2^1+2^0} \pmod{460} \\ &\equiv 1619^{2^8} 1619^{2^6} 1619^{2^4} 1619^{2^3} 1619^{2^2} 1619^{2^1} 1619^{2^0}. \end{aligned} \tag{11}$$

Enligt den upprepade kvadreringen i ekvation 10 kan sista kongruensen i ekvation 11 nu skrivas i termer av x_i, $i = 0, 1, \ldots, 8$. Nästa steg är att multiplicera ihop dessa faktorer parvis, från vänster till höger, för att hela tiden hålla dem mindre än 460^2. Vi får

$$\begin{aligned}
1619^{351} &\equiv x_8x_6x_4x_3x_2x_1x_0 \pmod{460} \\
&\equiv 361 \cdot 301 \cdot 261 \cdot 381 \cdot 121 \cdot 81 \cdot 239 \\
&\equiv 101 \cdot 261 \cdot 381 \cdot 121 \cdot 81 \cdot 239 \\
&\equiv 141 \cdot 381 \cdot 121 \cdot 81 \cdot 239 \\
&\equiv 361 \cdot 121 \cdot 81 \cdot 239 \\
&\equiv 441 \cdot 81 \cdot 239 \\
&\equiv 301 \cdot 239 \\
&\equiv 179.
\end{aligned}$$

Alltså

$$1619^{351} \equiv 179 \pmod{460}.$$

(f) Jag skulle börja med att kontrollera de enkla reglerna för delbarhet; 461 är inte delbart med 2 eftersom sista siffran är udda, det är inte delbart med 3 eftersom siffersumman $4 + 6 + 1 = 11$ inte är det och det är inte heller delbart på 5 eftersom sista siffran inte är en 0:a eller en 5:a. Sedan skulle jag hitta den kvadrat som är närmast 461. $461 < 484 = 22^2$. Alltså behöver vi bara kontrollera primtal upp till det största primtalet mindre än 22, ty om 461 inte är ett primtal har det en unik primtalsfaktorisering som innehåller primtal skilda från 461, enligt Aritmetikens Fundamentalsats. Minst ett av dessa tal måste vara mindre än $\sqrt{461}$, ty skulle två primtal större än $\sqrt{461}$ ingå i faktoriseringen skulle vi få ett tal större än 461. Det största primtalet mindre än 22 är 19, så det sista steget är att manuellt kontrollera om 461 är delbart med primtalen mellan (inklusive) 7 och 19, (7, 11, 13, 17, 19), genom att helt enkelt försöka utföra divisionerna.

(g)

(h)

2 Fråga 2

3 Fråga 3

I samarbete med Erik Dahllöf.

(i)

$$\begin{aligned} G(x,y) &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} c_{n,k}x^n y^k \\ &= \sum_{n=0}^{\infty} x^n \left(\sum_{k=1}^{\infty} \left(c_{n,k}y^k\right) + \overbrace{c_{n,0}}^{=1} \right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} \left(c_{n,k}y^k x^n\right) + x^n \right) \end{aligned}$$

Eftersom serien ovan är absolutkonvergent går det att dela upp den inre summan enligt

$$G(x,y) = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} \left(c_{n,k}y^k x^n\right) \right) + \overbrace{\sum_{n=0}^{\infty} x^n}^{=\frac{1}{1-x}}.$$

Då $c_{0,k} = 0 \,\forall\, k > 0$, och vi börjar från $k = 1$ kan vi byta index så att serien börjar från $n = 1$ istället, utan att ändra något. Detta ger

$$\begin{aligned} G(x,y) &= \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} \left(c_{n,k}y^k x^n\right) \right) + \frac{1}{1-x} = \{c_n = c_{n-1,k} + c_{n-1,k-1}\} = \\ &= \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} \left(c_{n-1,k} + c_{n-1,k-1}\right) y^k x^n \right) + \frac{1}{1-x} \\ &= \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} c_{n-1,k}y^k x^n + \sum_{k=1}^{\infty} c_{n-1,k-1}y^k x^n \right) + \frac{1}{1-x} \\ &= \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} c_{n-1,k}y^k x^n + \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} c_{n-1,k-1}y^k x^n + \frac{1}{1-x}. \end{aligned}$$

Betrakta nu den första serien i uttrycket

$$\begin{aligned}
\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} c_{n-1,k}y^k x^n &= \sum_{n=1}^{\infty} x^n \sum_{k=1}^{\infty} c_{n-1,k}y^k \\
&= x\sum_{n=1}^{\infty} x^{n-1} \sum_{k=1}^{\infty} c_{n-1,k}y^k \\
&= x\sum_{n=0}^{\infty} x^{n} \sum_{k=1}^{\infty} c_{n,k}y^k \\
&= x\sum_{n=0}^{\infty} x^{n} \left(\sum_{k=0}^{\infty} \left(c_{n,k}y^k\right) - \overbrace{c_{n,0}}^{=1} \right) \\
&= x\sum_{n=0}^{\infty} x^{n} \left(\sum_{k=0}^{\infty} \left(c_{n,k}y^k\right) - x^n \right) \\
&= x\left(\overbrace{\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} c_{n,k}y^k}^{=G(x,y)} - \overbrace{\sum_{n=0}^{\infty} x^n}^{=\frac{1}{1-x}} \right) \\
&= xG(x,y) - \frac{x}{1-x}.
\end{aligned}$$

Detta ger

$$\begin{aligned}
G(x,y) &= xG(x,y) - \frac{x}{1-x} + \overbrace{\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} c_{n-1,k-1}y^k x^n}^{=xyG(x,y)} + \frac{1}{1-x} \\
&= xG(x,y) + xyG(x,y) + 1.
\end{aligned}$$

Löser vi för $G(x,y)$ får vi

$$G(x,y) = \frac{1}{1-x-xy} \quad \textit{V.S.V.}$$

(ii) Enligt ovan är

$$\begin{aligned}
G(x,y) &= \frac{1}{1-x-xy} \\
&= \frac{1}{1-x(1+y)} \\
&= \sum_{n=0}^{\infty} \left(x(1+y)\right)^n \\
&= \sum_{n=0}^{\infty} \left(x^n \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} y^k \right).
\end{aligned}$$

Eftersom $\binom{n}{k} = 0 \, \forall \, k > n$ kan vi låta k gå till ∞ i den inre summan. Alltså får vi

$$\sum_{n=0}^{\infty} \left(x^n \sum_{k=0}^{\infty} \binom{n}{k} 1^{n-k} y^k \right) = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \binom{n}{k} x^n y^k$$

men detta är lika med $G(x, y)$, alltså

$$G(x,y) = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} c_{n,k} x^n y^k = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \binom{n}{k} x^n y^k$$
$$\implies c_{n,k} = \binom{n}{k} \quad V.S.V.$$

4 Fråga 4

5 Fråga 5

(i) Vill visa att $d_n = nd_{n-1} + (-1)^n \; \forall n \geq 1$ givet $d_0 = 1$. Testar vi basfallet $n = 1$ får vi $d_1 = 1d_0 - 1 = 0$, vilket stämmer överrens med ekvation 2 i uppgiftsbeskrivningen. Antag att rekursionen gäller i något fall $n = m$, alltså $d_m = md_{m-1} + (-1)^m$. Vi vill då visa att det även gäller i nästkommande fall $n = m + 1$, alltså $d_{m+1} = (m+1)d_m + (-1)^{m+1}$. Enligt ekvation 2 i uppgiften har vi att

$$\begin{aligned}
d_{m+1} &= (m + 1 - 1)(d_{m+1-1} + d_{m+1-2}) \\
&= m(d_m + d_{m-1}) \\
&= md_m + md_{m-1} \\
&= md_m + \overbrace{(md_{m-1} + (-1)^m)}^{= d_m \text{ enl. ant.}} - (-1)^m \\
&= md_m + d_m \overbrace{-(-1)^m}^{= +(-1)^{m+1}} \\
&= (m+1)d_m + (-1)^{m+1} \quad v.s.v.
\end{aligned}$$

(ii) Vi kan skriva manipulera $E(x)$ enligt

$$E(x) = \sum_{n=1}^{\infty} \frac{d_n}{n!} x^n + \overbrace{d_0}^{=1}$$
$$xE(x) = \sum_{n=0}^{\infty} \frac{d_n}{n!} x^{n+1} = \sum_{n=1}^{\infty} \frac{d_{n-1}}{(n-1)!} x^n = \sum_{n=1}^{\infty} \frac{nd_{n-1}}{n!} x^n.$$

Detta ger att

$$\begin{aligned}(1-x)E(x) &= \sum_{n=1}^{\infty}\left(\frac{d_n - nd_{n-1}}{n!}x^n\right) + 1 \\ &= \sum_{n=1}^{\infty}\left(\frac{(-1)^n}{n!}x^n\right) + 1 \\ &= \sum_{n=0}^{\infty}\left(\frac{(-1)^n}{n!}x^n\right)\end{aligned}$$

$$\implies E(x) = \frac{1}{1-x}\overbrace{\sum_{n=0}^{\infty}\frac{(-x)^n}{n!}}^{=e^{-x}} = \frac{e^{-x}}{1-x} \quad v.s.v.$$

(iii) Betrakta två potensserier $\sum_{n=0}^{\infty} a_n x_n$ och $\sum_{n=0}^{\infty} b_n x^n$. Om vi antar att båda serierna konvergerar absolut, så att vi slipper konvergensproblem, kan vi skriva upp en serie för deras produkt. Skriver vi ut de förstå termerna i produkten av serierna får vi

$$\begin{aligned}&\left(a_0 + a_1x^1 + a_2x^2 + \ldots\right)\left(b_0 + b_1x^1 + b_2x^2 + \ldots\right) = \\ =&a_0b_0 + \left(a_0b_1 + a_1b_0\right)x^1 + \left(a_0b_2 + a_1b_1 + a_2b_0\right)x^2 + \ldots.\end{aligned}$$

Detta ger att koefficienterna framrör x^n kommer vara

$$\sum_{k=0}^{n} a_k b_{n-k}.$$

Vilket ger att

$$\left(\sum_{n=0}^{\infty} a_n x_n\right)\left(\sum_{n=0}^{\infty} b_n x_n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n. \tag{12}$$

I vårt fall har vi

$$\begin{aligned}E(x) = \frac{e^{-x}}{1-x} &= \frac{1}{1-x}\sum_{n=0}^{\infty}\frac{(-x)^n}{n!} \\ &= \sum_{n=0}^{\infty}x^n\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}x^n.\end{aligned}$$

Använder vi likheten ekv. 12 med $a_n = 1\,\forall\, n \in \mathbb{N}$, $b_n = \frac{(-1)^n}{n!}\,\forall\, n \in \mathbb{N}$ får vi

$$E(x) = \sum_{n=0}^{\infty}x^n\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}x^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)x^n. \tag{13}$$

Men vi har att

$$E(x) = \sum_{n=0}^{\infty} \frac{d_n}{n!} x^n. \tag{14}$$

Gemför vi koefficienterna för x^n i ekv. 13 och 14 ser vi att

$$\frac{d_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad v.s.v.$$