4. *(Inledande talteori / Aritmetik)* Använd Euklides algoritm för att finna den multiplikativa inversen modulo 19 för 17 och använd den för att finna alla heltal x som uppfyller

$$17 \cdot x \equiv 22 \pmod{19}.$$

Alla tal i svaren ska vara reducerade modulo 19.

Lösning: Eftersom $22 \equiv 3 \pmod{19}$ gäller

$$17 \cdot x \equiv 22 \pmod{19} \Leftrightarrow 17 \cdot x \equiv 3 \pmod{19}$$

och vi löser denna enklare kongruens. Den multiplikativa inversen till 17 modulo 19 får vi med Euklides utvidgade algoritm enligt

$19 = 1 \cdot 17 + 2,$
$17 = 8 \cdot 2 + 1,$
$1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (19 - 17) = 9 \cdot 17 - 8 \cdot 19$

varav vi läser av kongruensen $9 \cdot 17 \equiv 1 \pmod{19}$ så att den multiplikativa inversen till 17 modulo 19 är **9**. Nu fås lösningen till $17 \cdot x \equiv 3 \pmod{19}$ genom multiplikation med den multiplikativa inversen så att vi har

$$17 \cdot x \equiv 3 \pmod{19} \Leftrightarrow 9 \cdot 17 \cdot x \equiv 9 \cdot 3 \pmod{19} \Leftrightarrow 1 \cdot x \equiv 27 \pmod{19} \Leftrightarrow x \equiv 8 \pmod{19}$$

som alltså är svaret.

5. *(Relationer)* Definiera relationen $\mathcal{R}$ på mängden av alla heltal $\mathbb{Z}$ genom

$$x\mathcal{R}y \Leftrightarrow (x-1) \cdot (y-1) \text{ är ett jämnt tal.}$$

Utred vilka egenskaper denna relation har av *reflexivitet*, *symmetri*, *anti-symmetri* och *transitivitet*. Om relationen har en viss egenskap ge ett bevis för den egenskapen. Om relationen *inte* har en viss egenskap, visa då att den inte har denna egenskap genom att visa den logiska motsatsen till att relationen uppfyller definitionen för egenskapen ifråga. Utredningen ska täcka samtliga fyra egenskaper.

Lösning: Vi studerar egenskaperna var för sig.

Reflexivitet: Relationen är **inte reflexiv** eftersom vi kan hitta tal x som *inte* uppfyller $x\mathcal{R}x$, till exempel gäller detta för talet $x = 2$, vi har *inte* att $2\mathcal{R}2$ eftersom

$$(2-1) \cdot (2-1) = 1$$

och talet 1 är inte ett jämnt tal.

Symmetri: Relationen **är symmetrisk**. Studera nämligen två godtyckliga heltal x, y med $x\mathcal{R}y$. Då har vi

$$x\mathcal{R}y \Leftrightarrow (x-1) \cdot (y-1) \text{ jämnt} \Leftrightarrow (y-1) \cdot (x-1) \text{ jämnt} \Leftrightarrow y\mathcal{R}x$$

och denna ekvivalens uttrycker precis egenskapen symmetri. (Det hade räckt med implikation.)

Anti-symmetri: Relationen är **inte anti-symmetrisk**, till exempel har vi $1\mathcal{R}2$ och $2\mathcal{R}1$ eftersom

$$(1-1) \cdot (2-1) = (2-1) \cdot (1-1) = 0 \text{ som är jämnt}$$

men $1 \neq 2$. Vi har alltså hittat ett motexempel på kravet som måste vara uppfyllt för alla heltal för att vi ska ha anti-symmetri.

Transitivitet: Faktiskt duger exemplet ovan också för att visa att relationen **inte är transitiv**. Vi har, enligt ovan, $1\mathcal{R}2$ och $2\mathcal{R}1$ och transitiviteten kräver då att $1\mathcal{R}1$, men som vi såg ovan (under *reflexivitet*) gäller inte $1\mathcal{R}1$. (Transitivitet kräver ju att $xRy \wedge yRz \rightarrow xRz$ och detta gäller alltså inte för $x = z = 1$ och $y = 2$.)

6. *(Fördjupad Talteori)* Använd matematisk induktion för att bevisa att $7^n - 4^n$ är delbart med 3 för alla positiva heltal n.

Lösning: Inför predikatet $A(n) \Leftrightarrow 3|7^n - 4^n$. Vi ska visa $\forall n \in \mathbb{N} : A(n)$. ($\mathbb{N} = \{1, 2, 3, \ldots\}$.)

Steg 1. Visa att $A(1)$ är sann. Men det gäller trivialt eftersom $A(1) \Leftrightarrow 3|7^1 - 4^1 \Leftrightarrow 3|3$.

Steg 2. Visa nu att implikationen $A(p) \Rightarrow A(p+1)$ alltid är sann för alla $p \in \mathbb{N}$. Låt alltså p vara godtyckligt i $\mathbb{N}$.

(a) Gör induktionsantagandet $A(p) \Leftrightarrow 3|7^p - 4^p$. Detta kan skrivas $\exists k \in \mathbb{Z} : 7^p - 4^p = 3 \cdot k$. Med kraft av detta ska vi visa att $A(p+1)$ är sann.

(b) Arbeta nu med utsagan $A(p+1)$. Den kan skrivas

$$\exists m \in \mathbb{Z} : 7^{p+1} - 4^{p+1} = 3 \cdot m$$

och vi vill visa att den är sann med hjälp av induktionsantagandet. Vi skriver därför om induktionsantagandet enligt

$$\exists k \in \mathbb{Z} : 7^p - 4^p = 3 \cdot k \Leftrightarrow \exists k \in \mathbb{Z} : 7^p = 3 \cdot k + 4^p.$$

Så vi kan alltså skriva om 7^p, detta använder vi och får:

$$7^{p+1} - 4^{p+1} = 7 \cdot 7^p - 4 \cdot 4^p = 7 \cdot (3 \cdot k + 4^p) - 4 \cdot 4^p = 3 \cdot 7 \cdot k + 7 \cdot 4^p - 4 \cdot 4^p$$

men detta kan skrivas som $= 3 \cdot (7k + 4^p)$ som klart är delbart med 3, och vi har alltså att $\exists m \in \mathbb{Z} : 7^{p+1} - 4^{p+1} = 3 \cdot m$ gäller med $m = 7k + 4^p$. $A(p+1)$ är alltså sann.

(c) Vi drar från detta slutsatsen $A(p) \Rightarrow A(p+1)$ för alla $p \in \mathbb{N}$ vilket fullbordar steg 2 i beviset.

Steg 3. Vi har alltså $A(1)$ sann $\Rightarrow A(2)$ sann $\Rightarrow A(3)$ sann och så vidare så att $\forall n \in \mathbb{N} : A(n)$ gäller och detta följer alltså av steg 1 och 2 och induktionsaxiomet. (Också kallat ”principen för matematisk induktion”.) Beviset är klart.

Anmärkning: Studenter frågar ibland om det är tvunget att skriva så mycket och svaret är nej, men motiveringen måste ändå vara *fullständig* – alltså inga led som behövs för att dra den slutsats vi vill dra får utelämnas.

När jag skriver ner en lösning är främsta målet att ge en förklaring snarare än ett kortfattat bevis. Men det går förstås inte att var hur kortfattad som helst. En minimal formulering av steg 3 skulle kunna se ut så här:

”*Steg 3.* Steg 1 och steg 2 samt induktionsaxiomet fullbordar beviset.”