Uppgift A.

Om $a \neq 0 \bmod m$ så har a en inverse mod m om och endast om $\gcd(a, m) = 1$.

Beteckna a's inverse mod m som a^{-1}.

Bestäm för alla olika a mod 15 om de har en inverse mod 15 och i fall a^{-1} finns bestäm dess värde.

a	a^{-1}	$\gcd(a,15)$
0	—	
1	1	1
2	8	1
3	—	3
4	4	1
5	—	5
6	—	3
7	13	1
8	2	1
9	—	3
10	—	5
11	11	1
12	—	3
13	7	1
14	14	1

Uppgift B

Beräkna $\gcd(a, m)$

			SVAR
i)	$m = 31$	$a = 24$	1
ii)	$m = 49$	$a = 11$	1
iii)	$m = 63$	$a = 14$	7
iv)	$m = 72$	$a = 8$	8
v)	$m = 143$	$a = 52$	13

Uppgift C.

Beräkna a^{-1} för a mod m där

i)	$m = 31$	$a = 24$
ii)	$m = 49$	$a = 11$
iii)	$m = 143$	$a = 32$

ii) $m = 31$, $a = 24$

$$31 = 1 \cdot 24 + 7.$$
$$24 = 3 \cdot 7 + 3.$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$
gcd.

$$\begin{aligned} 1 = 7 - 2 \cdot 3 &= 7 - 2(24 - 3 \cdot 7) \\ &= 7 - 2 \cdot 24 + 6 \cdot 7. \\ &= (1+6) \cdot 7 - 2 \cdot 24. \\ &= (1+6)(31 - 1 \cdot 24) - 2 \cdot 24. \\ &= 7 \cdot 31 - 7 \cdot 24 - 2 \cdot 24 \\ &= 7 \cdot 31 - 9 \cdot 24 \end{aligned}$$

$$\begin{aligned} 1 &= 7 \cdot 31 - 9 \cdot 24 \mod 31. \\ &= -9 \cdot 24 \mod 31 \\ &= (-9 \cdot 24 + 0) \mod 31 \\ &= (-9 \cdot 24 + 31 \cdot 24) \mod 31 \\ &= (31 - 9) \cdot 24 \mod 31 \\ &= (22) 24 \mod 31 \end{aligned}$$

$$\Rightarrow 24^{-1} = 22. \mod 31$$

kontroll $24 \cdot 22 = 528 = 17 \cdot 31 + 1$

ii) $m = 49 \quad a = 11$

$$49 = 4 \cdot 11 + 5$$

$$\left.\begin{aligned} 11 &= 2 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}\right\} \text{gcd.}$$

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2(49 - 4 \cdot 11) \\ &= (1 + 8 \cdot)11 - 2 \cdot 49 \\ &= 9 \cdot 11 - 2 \cdot 49 \end{aligned}$$

$$\begin{aligned} 1 &= 9 \cdot 11 - 2 \cdot 49 \mod 49 \\ &= 9 \cdot 11 - 0 \mod 49. \\ &= 9 \cdot 11 \mod 49 \end{aligned}$$

$$\Rightarrow a^{-1} = 11^{-1} = 9 \mod 49$$

kontroll $\quad 9 \cdot 11 = 99 = 2 \cdot 49 + 1$

(ii) $m = 143 \quad a = 32.$

$$143 = 4 \cdot 32 + 15$$
$$32 = 2 \cdot 15 + 2.$$
$$15 = 7 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$
gcd ok.

$$\begin{aligned}
1 &= 15 - 7 \cdot 2 \\
&= 15 - 7 \cdot (32 - 2 \cdot 15) \\
&= (1 + 14)15 - 7 \cdot 32. \\
&= 15 \cdot 15 - 7 \cdot 32. \\
&= 15(143 - 4 \cdot 32) - 7 \cdot 32. \\
&= 15 \cdot 143 - 60 \cdot 32 - 7 \cdot 32 \\
&= 15 \cdot 143 - 67 \cdot 32
\end{aligned}$$

$$\begin{aligned}
1 &= 15 \cdot 143 - 67 \cdot 32 \mod 143. \\
&= -67 \cdot 32 \mod 143 \\
&= (143 - 67) \cdot 32 \mod 143 \\
&= 76 \cdot 32 \mod 143 \quad \Rightarrow \quad 32^{-1} = 76 \mod 143
\end{aligned}$$

kontroll $\quad 76 \cdot 32 = 2432 = 17 \cdot 143 + 1$