

Övningsks 4.

1) (För varje delfråga ger rätt svar $\frac{1}{2}$ p, inget svar 0p, fel svar $-\frac{1}{2}$ p.
Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)
Kryssa för om påståendena **a)–f)** är sanna eller falska (eller avstå)!

	sant	falskt
a) Om grupperna G_1 och G_2 är isomorfa så är de lika stora.		
b) Sidoklasser till en och samma delgrupp H till en grupp G är lika stora.		
c) Om elementet g i en grupp G med gruppoperationen $\circ$ har ordning 20 så har elementet $g \circ g$ ordning 10.		
d) Om en ändlig grupp G verkar på mängden X och $x \in X$ är antalet element i banan Gx en delare till $ G $.		
e) Ett RSA-krypto kan ha parametrarna $n = 46$ och $e = 2$.		
f) Ett RSA-krypto kan ha $d = 5$ och $e = 5$.		

- 2a) (1p) Låt gruppen G ha vidstående grupptabell.
Bestäm ett element x i G sådant att $bxc = f$.
- | $\circ$ | a | b | c | d | f |
|---------|-----|-----|-----|-----|-----|
| a | a | b | c | d | f |
| b | b | c | d | f | a |
| c | c | d | f | a | b |
- b) (1p) Du vill ha ett RSA-krypto med parametern $n = 65$. Ange ett möjligt värde på parametern e .
- | $\circ$ | a | b | c | d | f |
|---------|-----|-----|-----|-----|-----|
| d | d | f | a | b | c |
| f | f | a | b | c | d |
- c) (1p) Formulera "Burnsides lemma", en formel för antalet banor då en ändlig grupp G verkar på en mängd X . Förklara kortfattat ingående beteckningar.

3) (3p) Betrakta gruppen $(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$. Avgör om denna grupp genereras av elementet 2.

4) (3p) Ett RSA-krypto har de offentliga nycklarna $n = 39$ och $e = 11$. Bestäm parametern d och ange hur meddelande 2 kan dekrypteras, dvs ange hur $D(2)$ beräknas.

(Du behöver alltså inte beräkna $D(2)$ för att få full poäng på denna uppgift men du skall berätta hur man går till väga.)

5) (3p) Bestäm en delgrupp med tre element till den grupp G som har vidstående grupptabell:

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d