1d) Morda je za A najlažje izbrati kar
$A(p,q,r) = p \vee q \vee r$
V tem primeru nabor $\{A, \vee\}$ ne more izraziti kaj več od disjunkcije.

1e) Vemo, da je, denimo, $\{\uparrow\}$ poln nabor. Če s trometrim veznikom B izrazimo $\uparrow$, potem smo zmagali.
Morda kliče je $B(p,q,r) = p \uparrow (q \wedge r) \sim \neg(p \wedge q \wedge r)$
V tem primeru je sveda $B(p,q,q) \sim p \uparrow (q \wedge q) \sim p \uparrow q$
Pari pa na tole.
$$p \uparrow q \uparrow r \sim (p \uparrow q) \uparrow r \not\sim \neg(p \wedge q \wedge r)$$
Vemo $\overline{B}(p,q,r) = p \uparrow q \uparrow r$ namreč ohranja logično vrednost 1, saj je
$$\overline{B}(1,1,1) \sim (1 \uparrow 1) \uparrow 1 \sim \neg(\neg(1 \wedge 1) \wedge 1) \sim$$
$$\sim \neg(0 \wedge 1) \sim \neg 0 \sim 1$$

2c) Če A in B nista primerljiva (nobena od A, B ni podmnožica druge), potem zveza ne velja.
Če namreč $a \in A \setminus B$ in $b \in B \setminus A$, potem
$\{a,b\} \in \mathcal{P}(A \cup B)$, toda $\{a,b\} \notin \mathcal{P}A \cup \mathcal{P}B$.
Zveza $\mathcal{P}(A \cup B) = \mathcal{P}A \cup \mathcal{P}B$ velja za primerljive pare množic (tj. veljati mora $A \subseteq B$ ali $B \subseteq A$)
Če, denimo, velja $A \subseteq B$, potem je
- $A \cup B = B$ (in zato $\mathcal{P}(A \cup B) = \mathcal{P}B$) in
- $\mathcal{P}A \subseteq \mathcal{P}B$ (saj je vsaka podmnožica A vsekakor v B)

3c) Opozoriti je bilo potrebno drugje (za zato izbrisu a, b)
- $\gcd(a,b)$ <u>deli</u> a (oziroma a je večkratnik $\gcd(a,b)$)
zato je $\operatorname{lcm}(a, \gcd(a,b)) = a$
- a <u>deli</u> $\operatorname{lcm}(a,b)$ (oziroma $\operatorname{lcm}(a,b)$ je večkratnik a)
zato je $\gcd(a, \operatorname{lcm}(a,b)) = a$

3d, e) Ker sta 1 in p edina deljitelja števila p, lahko samo ti dve vrednosti zavzame izraz $\gcd(a,p)$.
- 1 takrat, ko je a tuj p in
- p takrat, ko p deli a.

Da se ni potrebno ločeno obravnavati obeh primerov, je najustreznje uporabiti drugi del Malega Fermatovega izreka, ki pravi, da je $a^p \equiv a \pmod p$

Zato je $a^{2p-1} \equiv a^p \cdot a^{p-1} \equiv a \cdot a^{p-1} \equiv a^p \equiv a \pmod p$

Pri del M.F.I. oz. E.I. pravita, da če je $a \perp p$, potem $a^{p-1} \equiv 1 \pmod p$.

To pomeni, da je treba primer "a ni tuj p" obravnavati ločeno.

4a) Parost permutacije lahko določimo iz ciklične strukture (seštevamo za 1 zmanjšane dolžine ciklov), red pa tudi (iščemo lcm dolžin ciklov).

Permutacija s c.s. $[5,2]$ je liha, njen red pa je 10.

Sodo permutacijo pa lahko dobimo, če za c.s. izberemo $[5,5,2,2]$. ← Sicer je potrebno napisati tudi zgleda

4c) 16 je potenca praštevila in če raj ima permutacija red 16, potem mora v njeni ciklični strukturi vsebovati 16-cikel.

Žal je permutacija s c.s. $[16]$ liha. Soda permutacija s c.s. $[16,2]$ je soda in ravno želenega reda 16.

4a in c lahko rešimo tudi z drugačnima argumentoma.

Tudi permutacija s c.s. $[5,2,2]$ je soda in je njen red enak 10.

In tudi permutacija s c.s. $[16,16]$ je soda in ima red enak 16.