[12.15] $A = \{n \in \mathbb{Z}_+ : 2 \le n \le 2000\}$ po-mängd $(A, |)$.

a) Lattice? $\{1999, 2000\}$ det största finns

möb $\{1999, 2000\}$ och sub $\{1999, 2000\}$ finns inte

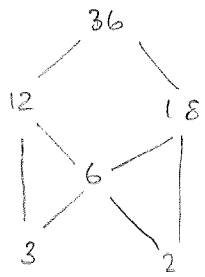
a Maximal om det inte finns $x \in A$ med $x \neq a$, $a \mid x$ $(x = ka, k \in \mathbb{Z})$

$a \geq 1001$ är a maximal det finns 1000 sådana tal

Dvs. a kan inte dela någonting,

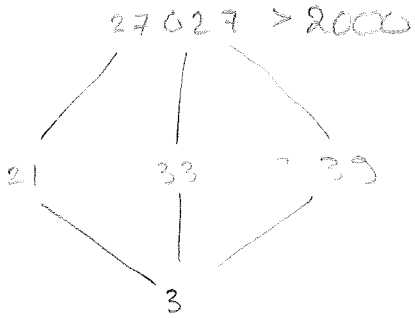
b) möb $\{12, 18\} = 36$

sub $\{12, 18\} = 6$



c) möb $\{21, 33, 39\}$?

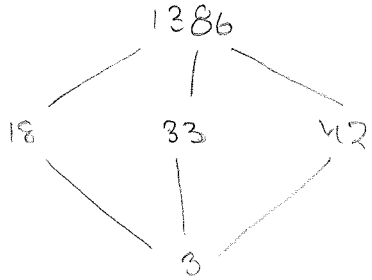
saknas



sub $\{21, 33, 39\} = 3$

d) möb $\{18, 33, 42\} = 1386$

sub $\{18, 33, 42\} = 3$



e) ? ? ? Hur ta reda på?

f) Primtallen i A!

Lektion 8

[6.3]

visa att $3 \mid 7^n - 4^n \quad \forall\, n \in \mathbb{N}$

Induktionsbas:

$3 \mid 7^1 - 4^1 \Rightarrow 3 \mid 3$ ok

Induktionsantagande:

$7^p - 4^p = 3k \quad \Rightarrow \quad 7^p = 3k + 4^p$

induktionssteg:

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

$21k + 3 \cdot 4^p = 3(7k + 3 \cdot 4^p)$, detta visar att

$3 \mid 7^{p+1} - 4^{p+1}$

V.S.V

[6.6]

Låt p och q vara primtal. Visa att $p \mid q$ o.m.m $p = q$

om $p \mid q \Rightarrow pk = q \Rightarrow k = \frac{q}{p} \Rightarrow \{q \text{ och } p \text{ primtal}\} \Rightarrow$

$k = 1$ och $q = p$.

[6.20]

Bland 1, 2, 3, .., 200 väljs på måfå 101 tal. Visa att det bland dessa finns ett par tal som är sådant att det ena talet är delbart med det andra.

$ak = b$, $a, b \leq 200$, $k \in \mathbb{Z}^+$

alla tal $a \geq 101$ är sådana att $a \nmid b$, då $b > a$. Om dessa väljs är 100 tal valda. Genom att välja <u>ett till</u> får vi minst ett talpar sådant att $a | b$.

[6.26] n udda:

$8 | (n^2 - 1)$

$n^2 - 1 = \left\{ \begin{matrix} n = 4k+1 \\ k \in \mathbb{Z}^+ \end{matrix} \right\} = (4k+1)^2 - 1 = 16k^2 + 8k + 1 - 1 = 16k^2 + 8k =$

$= 8(2k^2 + k) \Rightarrow 8 | (n^2 - 1)$ N.S.U

[6.31]

$a, b \in \mathbb{Z}$ och $sgd(a,b) = d$. Visa att $sgd(\frac{a}{d}, \frac{b}{d}) = 1$

$$\begin{cases} a = kd \\ b = jd \end{cases} \Rightarrow sgd\left(\frac{a}{d}, \frac{b}{d}\right) = sgd\left(\frac{(kd)}{d}, \frac{(jd)}{d}\right) = sgd(k, j) = 1$$

[6.32]

a) om a udda $\Rightarrow$ $sgd(a-1, a+1) = 2$ visa:

$sgd(a-1, a+1) = \{a+1 = (a-1)\cdot 1 + 2\} =$

$sgd(a-1, 2) = \{a-1$ jämnt tal $\Rightarrow$ delbart med $2\} = 2$ v.s.v.

b) om a jämnt $\Rightarrow$ $sgd(a-1, a+1) = 1$ visa:

$sgd(a-1, a+1) = \{a+1 = (a-1)\cdot 1 + 2\} =$

$sgd(a-1, 2) = \{a-1$ udda tal, ej delbart med $2\} = 1$. v.s.v.

[6.37] största n som uppfyller $2^n \mid 30!$?

Dvs, hur många gånger kan man dela 30! med 2?

Tal	kan delas # ggr:		
30	1	rest	15
28	2	rest	7
26	1	rest	13
24	3	rest	3
22	1		11
20	2		5
18	1		9
16	3		2
14	1		7
12	2		3
10	1		5
8	2		2
6	1		3
4	2		1
2	1		1

2 ggr till...

24 ggr + 2 = 26 ggr

[6.36] Låt $n = 2^{12} \cdot 3^{8} \cdot 5^{6} \cdot 7^{2} \cdot 11^{4} \cdot 13^{3} \cdot 23 \cdot 151$

a) Antal delare (pos och neg):

exponenterna +1, varför +1?

$2 \cdot (13 \cdot 9 \cdot 7 \cdot 3 \cdot 5 \cdot 4 \cdot 2 \cdot 2) = 393120$

b) Pos. delare: $196560 = 13 \cdot 9 \cdot 7 \cdot 3 \cdot 5 \cdot 4 \cdot 2 \cdot 2$

c) $7 \times 5 \times 4 \times 2 \times 3 \times 2 = 1680$

d) $8 \cdot 6 \cdot 3 \cdot 1$.

e) $3 \cdot 4 \cdot 2 \cdot 2 \cdot 3$ varför 3??

[8.3]

a) 5^{1111} mod 12

$5^2 = 25 = 12 \cdot 2 + 1 \equiv 1$ mod 12

$5^4 = (5^2)^2 \equiv 25^2 \equiv 1^2 = 1$

$5^{1000} = (5^2)^{500} = 25^{500} \equiv 1^{500}$

$5^{100} = (5^2)^{50} = 25^{50} \equiv 1^{50}$

$5^{10} = (5^2)^5 = 25^5 \equiv 1^5$

$5^1 \equiv 5$

Ekv.klasser mod 12

[0] : {... -12, 0, 12, 24}

[1] : {... -11, 1, 13, 25 ...}

[2] : {... -10, 2, 14, 26 ...}

⋮

[5] : {... -7, 5, 17, 29 ...}

$5^{1111} = 5^{1000} \cdot 5^{100} \cdot 5^{10} \cdot 5^1 \equiv 1 \cdot 1 \cdot 1 \cdot 5 = 5$

svar: 5

b) 3^{41} mod 79

$3^4 = 9^2 = 81 \equiv 2$ mod 79

$3^8 = (3^4)^2 = (9^2)^2 \equiv 2^2 = 4$ mod 79

$3^{40} = (3^8)^5 \equiv 4^5 = 1024 = 79 \cdot 12 + 76 \equiv 76$

$3^{41} = 3^{40} \cdot 3^1 \equiv 76 \cdot 3 = 228 \equiv 79 \cdot 2 + 70 \equiv 70$

svar: 70

c) 4^{220} mod 19

$4^2 = 16 \equiv 16$

$4^4 = (4^2)^2 \equiv 16^2 = 256 = 19 \cdot 13 + 9 \equiv 9$

$4^8 = (4^4)^2 \equiv 9^2 = 81 = 19 \cdot 4 + 5 \equiv 5$

$4^{16} = (4^8)^2 \equiv 5^2 = 25 = 1 \cdot 19 + 6 \equiv 6$

$4^{32} = (4^{16})^2 \equiv 6^2 = 36 = 1 \cdot 19 + 17 \equiv 17$

$4^{64} = (4^{32})^2 \equiv 17^2 = 289 \equiv 4$

$4^{220} = \underbrace{4^{64} \cdot 4^{64} \cdot 4^{64}} \cdot 4^8 \cdot 4^4 \cdot 4^4 \cdot 4^4 \cdot 4^4 \cdot 4^4$

$\equiv 4^3 \cdot 5 \cdot 9^5$