Diffie Hellman key exchange

Og regning med rester...

Øvelser: Regning med rester

Regnestykke ☺	Facit
$17\ (mod\ 3)$	
$12\ (mod\ 3)$	
$24\ (mod\ 5)$	
$61\ (mod\ 11)$	
$53\ (mod\ 5)$	
$172\ (mod\ 35)$	
$2409\ (mod\ 19)$	
$5301\ (mod\ 71)$	

Facit: Regning med rester

Regnestykke ☺	Facit
$17\ (mod\ 3)$	2
$12\ (mod\ 3)$	0
$24\ (mod\ 5)$	4
$61\ (mod\ 11)$	6
$53\ (mod\ 5)$	3
$172\ (mod\ 35)$	32
$2409\ (mod\ 19)$	15
$5301\ (mod\ 71)$	47

Summe-øvelse

Lad a og n være hele tal.

- Hvilke værdier kan $a \ (mod \ 17)$ antage?
- Hvilke værdier kan $a \ (mod \ n)$ antage?

På jagt efter regneregler

- Udregn følgende udtryk

$(24 + 28)(mod\ 5)$	$\big(24\ (mod\ 5)\ + 28\ (mod\ 5)\big)(mod\ 5)$
$(24 \cdot 28)(mod\ 5)$	$\big(24\ (mod\ 5) \cdot 28\ (mod\ 5)\big)(mod\ 5)$
$7^4\ (mod\ 5)$	$\big(7\ (mod\ 5)\big)^4\ (mod\ 5)$
$(17 + 6 \cdot 5)(mod\ 5)$	$17\ (mod\ 5)$

- Hvad tænker du, der er nemmest at udregne for en computer: Venstre side eller højre side?

Regneregler

Sætning

Lad a og b være hele tal og lad n være et naturligt tal.
Da gælder:

$$1)\ (a+b)(mod\ n) = \big(a\ (mod\ n)\ + b\ (mod\ n)\big)(mod\ n)$$

$$2)\ (a \cdot b)(mod\ n) = \big(a\ (mod\ n) \cdot b\ (mod\ n)\big)(mod\ n)$$

$$3)\ a^t\ (mod\ n) = \big(a\ (mod\ n)\big)^t\ (mod\ n)$$

$$4)\ (a + k \cdot n)(mod\ n) = a\ (mod\ n)$$

De hele tal

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

De naturlige tal

$$\mathbb{N} = \{1, 2, 3, \dots\}$$