# 1 multiplikationstabellen mod 12

restklasser

1

$2 \cdot 6 = 0$

$3 \cdot 4 = 0$

$4 \cdot 3 = 0$

5

$6 \cdot 2 = 0$

7

$8 \cdot 3 = 0$

$9 \cdot 4 = 0$

$10 \cdot 6 = 0$

11

lämpliga kandidater

$1 \cdot 1 = 1$

$7 \cdot 7 = 49 = 1 \bmod 12$

$5 \cdot 5 = 25 = 1 \bmod 12$

$11 \cdot 11 = 121 = 1 \bmod 12$

mod 14 :

1

$2 \cdot 7 = 0$

3

$4 \cdot 7 = 0$

5

$6 \cdot 7 = 0$

$7 \cdot 2 = 0$

$8 \cdot 7 = 0$

9

$10 \cdot 7 = 0$

11

$12 \cdot 7 = 0$

13

kandidater

$1 \cdot 1 = 13 \cdot 13 = 1$

$3 \cdot 5 = 9 \cdot 11 = 1$

$\pmod{14}$

② $15x = 15 \pmod{35}$

$15x - 15$ är alltså delbart med 35.

$15x + 35y = 15$ – eller, annorlunda uttryckt

$3x + 7y = 3$

$3(x-1) = -7 \cdot y$

hjälpekv. $3x + 7y = 0$, $x = 7k$, $y = -3k$

part. lösn $x = 8$ $(y = -3)$

$\boxed{x = 8 + 7k}$

$14x = 7 \pmod{35}$

$14x - 7$ delb. med 35

$14x + 35y = 7$

$2x + 5y = 1$

$x = 3$ $(y = -1)$

$\boxed{x = 3 + 5k}$

$x = 8 + 7k \mod 35$

| | |
|---|---|
| $k=0$ | $x=8$ |
| $k=1$ | $x=15$ |
| $k=2$ | $x=22$ |
| $k=3$ | $x=29$ |
| $x=4$ | $x=1$ |

$x = 3 + 5k \mod 35$

| | |
|---|---|
| $k=0$ | $x=3$ |
| $k=1$ | 8 |
| 2 | 13 |
| 3 | 18 |
| 4 | 23 |
| 5 | 28 |
| 6 | 33 |

3. $n = 253 = 23 \cdot 11$

$p = 23$, $q = 11$

$m = (p-1)(q-1) = 220$

e var $= 3$.

$3d \equiv 1 \pmod{220}$

$3d - 1 = 440$ duger

$3d = 441$, $d = 147 = 128 + 16 + 2 + 1$

$2^{147} =$

$= 2^{128} \cdot 2^{16} \cdot 2^{2} \cdot 2$

$2^{\cdots}$ räknas

mha

successiv

kvadrering.

$n = 221 \quad p = 13, q = 17$

$m = (p-1)(q-1) = 12 \cdot 16 = 192$

$e = 5$

$5d \equiv 1 \pmod{192}$

$5d + 192y = 1;$

$192 = 38 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (192 - 38 \cdot 5)$

$77 = 64 + 8 + 4 + 1$

$2^{77} = 2^{64} \cdot 2^{8} \cdot 2^{4} \cdot 2$

$d = 77$