SI-PASS 4 – facit

1.

$SGD(663{,}294)$
$663 = 2 \cdot 294 + 75$
$294 = 3 \cdot 75 + 69$
$75 = 1 \cdot 69 + 6$
$69 = 11 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$
$SGD = 3$

2.

Först kör vi Euklides för att hitta SGD(55,38)

$55 = 38 + 17$
$38 = 2 \cdot 17 + 4$
$17 = 4 \cdot 4 + 1$

Sedan kör vi den åt motsatt håll

$1 = 17 - 4 \cdot 4$
$17 - 4 \cdot (38 - 2 \cdot 17) = 9 \cdot 17 - 4 \cdot 38$
$9 \cdot (55 - 38) - 4 \cdot 38$
$9 \cdot 55 - 13 \cdot 38$
$60 = 60 \cdot 9 \cdot 55 - 60 \cdot 13 \cdot 38$
$540 \cdot 55 - 780 \cdot 38$

$X_0 = -780$
$Y_0 = 540$

$$X = X_0 \pm n\left(\frac{55}{SGD(38{,}55)}\right) = -780 \pm 55n$$

$$Y = Y_0 \mp n\left(\frac{38}{SGD(38{,}55)}\right) = 540 \mp 38n$$

3.

$3^{336} (mod\, 7)$
$(3^2)^{168} (mod\, 7)$
$9^{168} (mod\, 7)$
$2^{168} (mod\, 7)$ Eftersom $2 \equiv 9\, (mod\, 7)$
$8^{56} (mod\, 7)$
$1^{56} (mod\, 7)$
$1 (mod\, 7)$

4.
Basfall:
$8^1 - 3^1 = 5 \equiv 0 \pmod{5}$
Antag att $5 | 8^n + 3^n$
$8^{n+1} - 3^{n+1} = 8 \cdot 8^n - 3 \cdot 3^n$
$3 \cdot 8^n + 5 \cdot 8^n - 3 \cdot 3^n$
$3(8^n - 3^n) + 5 \cdot 8^n$
$5 | 8^n - 3^n$ gäller samt $5 | 5 \cdot 8^n$
VSV

5.
$10n \equiv 1 \pmod{13}$
$13 = 10 + 3$
$10 = 3 \cdot 3 + 1$
$1 = 10 - 3 \cdot 3$
$10 - (13 - 10) \cdot 3 = 4 \cdot 10 - 13 * 3 = 1$
$n = 4$