

Solutions to Selected Exercises, HW #12

Assignment: Notes on the RSA Algorithm, Part F.

1. (a) $\gcd(5005, 210) = 35$.
(b) $5005 \cdot (-1) - 210 \cdot (-24) = 35$.
2. (a) $\gcd(234, 432) = 18$.
(b) $234 \cdot (-11) - 432 \cdot (-6) = 18$.
3. (a) $\varphi(143) = \varphi(11 \cdot 13) = 10 \cdot 12 = 120$.
(b) $\gcd(k, \varphi(143)) = \gcd(19, 120) = 1$.
(c) $19 \cdot 19 - 120 \cdot 3 = 1$.
(d) W.
4. (a)

$$\begin{aligned}120 &= 17 \cdot 7 + 1 \\17 &= 1 \cdot 17 + 0,\end{aligned}$$

$$\text{so } \gcd(17, 120) = 1.$$

- (b) $1 = 120 - 17 \cdot 7 = 17 \cdot (-7) - 120 \cdot (-1)$.
(c)

$$\begin{aligned}1 &= 17 \cdot (-7 + 120) - 120 \cdot (-1 + 17) \\1 &= 17 \cdot 113 - 120 \cdot 16\end{aligned}$$

- (d) 113.