1. Computing orders in U_7 we look for primitive elements (those of order $\varphi(7) = 6$)

```
? for(k=1,6,print("ord(",k,")=",znorder(Mod(k,7))))
ord(1)=1
ord(2)=3
ord(3)=6
ord(4)=3
ord(5)=6
ord(6)=2
```

   Therefore, 3 and 5 are generators of U_7. For example,

```
? for(k=1,6,print("3^",k,"=",Mod(3,7)^k))
3^1=Mod(3, 7)
3^2=Mod(2, 7)
3^3=Mod(6, 7)
3^4=Mod(4, 7)
3^5=Mod(5, 7)
3^6=Mod(1, 7)
```

   Computing the orders of elements of $U_8 = \{1, 3, 5, 7\}$ we find no elements of order 4 (other than 1 they have order 2), so U_8 is not cyclic.

2. In U_{13} we have $3^2 = 9$, $3^3 = 1$, so the subgroup generated by 3 is $H = \{1, 3, 9\}$. By Lagrange's theorem there are 4 distinct cosets $H = \{1, 3, 9\}$, $2H = \{2, 6, 5\}$, $4H = \{4, 12, 10\}$, $7H = \{7, 8, 11\}$.

3. $\ker f = \{0, 3, 6, 9, 12\}$ and the image is $\{0, 5, 10\}$. Both are subgroups of $\mathbf{Z}_{15}$, the kernel generated by 3 and the image by 5.

4. The second congruence implies the first, so we are reduced to solving $x \equiv 5 \bmod 8$, $x \equiv 3 \bmod 5$, where the two moduli are relatively prime. Following the book's notation we have $a_1 = 5$, $m_1 = 8$, $k_1 = 5$, $a_2 = 3$, $m_2 = 5$, $k_2 = 8$. To obtain multiplicative inverses we need a Bezout relation. Euclid's algorithm gives $8 = 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$. Solving for remainders we get $3 = 8 - 5$, $2 = 5 - 3$, $1 = 3 - 2$. Back substitution gives $1 = 3-2 = 3-(5-3) = 2\cdot3-5 = 2(8-5)-5 = 2\cdot8-3\cdot5$. Thus, the multiplicative inverses of k_i modulo m_i are $r_1 = -3$, $r_2 = 2$, so by the Chinese Remainder Theorem we have the unique (modulo m_1m_2) solution $x = a_1k_1r_1+a_2k_2r_2 = -5\cdot5\cdot3+3\cdot8\cdot2 = -27 \equiv 13 \bmod 40$.

   Check: $13 \equiv 5 \bmod 8$ and $13 \equiv 3 \bmod 5$.

5. By long division $x^3 - x = x(x^2 - 1) + x - 1$. Since $x - 1$ divides $x^2 - 1$, the gcd is $x - 1$. To obtain a Bezout relation, solve for the remainder $x - 1 = (x^3 - 1) - x(x^2 - 1)$.