Nick Roper

1)
a)
Suppose $a \equiv b \mod n$.
Thus, for some integer k, $a = kn + b$.
Therefore, $b = -kn + a$, so $b = (-k)n + a$.
Since $-k$ is an integer, $b \equiv a \mod n$.
Thus, $a \equiv b \mod n \implies b \equiv a \mod n$.

b)
Suppose $a \equiv b \mod n$ and $b \equiv c \mod n$.
Thus, for some integers k_1 and k_2, $a = k_1 n + b$ and $b = k_2 n + c$.
Therefore, $a = k_1 n + (k_2 n + c) = k_1 n + k_2 n + c = (k_1 + k_2)n + c$.
Since $k_1 + k_2$ is an integer, $a \equiv c \mod n$.
Thus, $(a \equiv b \mod n$ and $b \equiv c \mod n) \implies a \equiv c \mod n$.

2)
a)
$x_0 = 1, y_0 = 0$
$m = 4321, n = 1234$
$x_1 = 0, y_1 = 1$
$m = 1234, n = 619, q = 3$
$x_2 = 1, y_2 = -3$
$m = 619, n = 615, q = 1$
$x_3 = -1, y_3 = 4$
$m = 615, n = 4, q = 1$
$x_4 = 2, y_4 = -7$
$m = 4, n = 3, q = 153$
$x_5 = -307, y_5 = 1075$
$m = 3, n = 1, q = 1$
$x_6 = 309, y_6 = -1082$
$m = 1, n = 0, q = 3$
Thus, $1234^{-1} \equiv -1082 \mod 4321$,
so $1234^{-1} \equiv 3239 \mod 4321$.

b)
They clearly at least share a factor of 2, so $gcd(40902, 24140) \neq 1$, so the multiplicative inverse does not exist.
Extended euclidean algorithm anyways:
$x_0 = 1, y_0 = 0$
$m = 40902, n = 24140$
$x_1 = 0, y_1 = 1$

$m = 24140, n = 16762, q = 1$
$x_2 = 1, y_2 = -1$
$m = 16762, n = 7378, q = 1$
$x_3 = -1, y_3 = 2$
$m = 7378, n = 2006, q = 2$
$x_4 = 3, y_4 = -5$
$m = 2006, n = 1360, q = 3$
$x_5 = -10, y_5 = 17$
$m = 1360, n = 646, q = 1$
$x_6 = 13, y_6 = -22$
$m = 646, n = 68, q = 2$
$x_7 = -36, y_7 = 61$
$m = 68, n = 34, q = 9$
$x_8 = 337, y_8 = -571$
$m = 34, n = 0, q = 2$
Thus, we can see that $gcd(40902, 24140) = 34$,
so -571 is not the multiplicative inverse of 24140,
rather $(-571 \times 24140) \equiv 34 \mod 40902$.

c)
$x_0 = 1, y_0 = 0$
$m = 1769, n = 550$
$x_1 = 0, y_1 = 1$
$m = 550, n = 119, q = 3$
$x_2 = 1, y_2 = -3$
$m = 119, n = 74, q = 4$
$x_3 = -4, y_3 = 13$
$m = 74, n = 45, q = 1$
$x_4 = 5, y_4 = -16$
$m = 45, n = 29, q = 1$
$x_5 = -9, y_5 = 29$
$m = 29, n = 16, q = 1$
$x_6 = 14, y_6 = -45$
$m = 16, n = 13, q = 1$
$x_7 = -23, y_7 = 74$
$m = 13, n = 3, q = 1$
$x_8 = 37, y_8 = -119$
$m = 3, n = 1, q = 4$
$x_9 = -171, y_9 = 550$
$m = 1, n = 0, q = 3$
Thus, $550^{-1} \equiv 550 \mod 1769$.

3)
a)

x^3+1 can be factored into $(x+1)(x^2-x+1) \equiv (x+1)(x^2+x+1) \mod 2$, so x^3+1 is reducible over GF(2).

b)
x^3+x^2+1 is irreducible $\mod 2$,
so x^3+x^2+1 is not reducible over GF(2).

c)

$(x^2+1)(x^2+1) \equiv x^4+2x^2+1 \equiv x^4+1 \mod 2$,
so x^4+1 is reducible over GF(2).

4)
a)
After long division of x^3-x+1 by x^2+1 in GF(2),
$x^3-x+1 \equiv x(x^2+1)+1 \mod 2$.
Then, after long division of x^2+1 by 1 in GF(2),
$x^2+1 = 1(x^2+1)+0 \mod 2$.
Thus, the gcd of x^3-x+1 and x^2+1 is 1 in GF(2).

b)
After long division of $x^5+x^4+x^3-x^2-x+1$ by x^3+x^2+x+1 in GF(3),
$x^5+x^4+x^3-x^2-x+1 \equiv x^2(x^3+x^2+x+1)-2x^2-x+1 \mod 3$.
Then, after long division of x^3+x^2+x+1 by $-2x^2-x+1$ in GF(3),
$x^3+x^2+x+1 \equiv (-2x+2)(-2x^2-x+1)+2x-1 \mod 3$.
Then, after long division of $-2x^2-x+1$ by $2x-1$ in GF(3),
$-2x^2-x+1 \equiv (-x-1)(2x-1)+0 \mod 3$.
Thus, the gcd of $x^5+x^4+x^3-x^2-x+1$ and x^3+x^2+x+1 is $-x-1$ in GF(3).

5)
The key and the ciphertext do not determine the plaintext uniquely, so we compute $H(K|C)$ using the formula

$$H(X|Y) = -\sum_x \sum_y p(y) \cdot p(x|y) \log_2 p(x|y)$$

$p(c=1) = \frac{3}{8} + \frac{1}{8} = \frac{1}{2}$

$p(c=2) = \frac{1}{16} + \frac{1}{8} + \frac{1}{16} = \frac{1}{4}$

$p(c=3) = \frac{1}{16} + \frac{1}{16} = \frac{1}{8}$

$p(c = 4) = \frac{1}{8}$

$p(k_1|c = 1) = \frac{3}{4}$
$p(k_2|c = 1) = \frac{1}{4}$
$p(k_3|c = 1) = 0$
$p(k_1|c = 2) = \frac{1}{4}$
$p(k_2|c = 2) = \frac{1}{2}$
$p(k_3|c = 2) = \frac{1}{4}$
$p(k_1|c = 3) = 0$
$p(k_2|c = 3) = \frac{1}{2}$
$p(k_3|c = 3) = \frac{1}{2}$
$p(k_1|c = 4) = 0$
$p(k_2|c = 4) = 0$
$p(k_3|c = 4) = 1$
so, we can compute as:
$H(K|C) = -(\frac{1}{2}\left(\frac{3}{4}\log_2\left(\frac{3}{4}\right) + \frac{1}{4}\log_2\left(\frac{1}{4}\right)\right)$
$+ \frac{1}{4}\left(\frac{1}{4}\log_2\left(\frac{1}{4}\right) + \frac{1}{2}\log_2\left(\frac{1}{2}\right) + \frac{1}{4}\log_2\left(\frac{1}{4}\right)\right)$
$+ \frac{1}{8}\left(\frac{1}{2}\log_2\left(\frac{1}{2}\right) + \frac{1}{2}\log_2\left(\frac{1}{2}\right)\right)$
$+ \frac{1}{8}\left(1\log_2\left(1\right)\right))$
≈ 0.9056

$H(K|C) \approx 0.9056$