Solution to Tom Weston's Practice Exam 1:

Problem 1: See solution to Sec 3.1 page 96 Problem 13 on our HW web page.

Prob 2:

(a) $176x + 143y = 17$

Step 1: Find $\gcd(176, 143)$ and solve $176x + 143y = \gcd(176, 143)$

$176x_i + 143y_i = r_i$

x_i	y_i	r_i	q_i
1	0	176	–
0	1	143	
1	−1	33	1
−4	5	11	4

$\gcd(176, 143) = 11$

$$\boxed{176\cdot(-4) + 143\cdot 5 = 11}$$

Step 2:

Now $11 \nmid 17$. Hence, the Diophantine Eq (a) does not have a solution.

(b) $176x + 143y = -44 = -4\cdot 11$

$(x_0, y_0) = -4(-4, 5) = (16, -20)$ is a particular solution. The general solution is

$$\left\{(x,y) = \left(16 - \frac{143}{11}k, -20 + \frac{176}{11}k\right) : k \in \mathbb{Z}\right\}.$$

(c) $101x + 47y = 19$

Step 1:

Solve $101x + 47y = \gcd(101, 47)$

$101 x_i + 47 y_i = r_i$

x_i	y_i	r_i	q_i
1	0	101	—
0	1	47	—
1	-2	7	2
-6	13	5	6
7	-15	2	1
-20	43	1	2
		0	

$\gcd(101, 47)$

$$\boxed{101(-20) + 47 \cdot 43 = 1}$$

Step 2: A particular sol'n to (c) is

$(x_0, y_0) = 19 \cdot (-20, 43) = (-38, 817)$

The general solution is

$\{(x, y) = (-38 - 47k, 817 + 101k) : k \in \mathbb{Z}\}$.

Problem 3: Find all solutions to the Diophantine Equation $7x + 9y = 120$ (*) with $x, y \in \mathbb{N}$.

Answer: First find a particular sol'n to $7x + 9y = 1$

$9y_i + 7x_i = r_i$

y_i	x_i	r_i	q_i
1	0	9	—
0	1	7	—
1	−1	2	1
−3	4	1	3
		0	

$7(4) + 9(-3) = 1$

So $(x_0, y_0) := 120(4, -3) = (480, -360)$ is a particular sol'n of (*). The general sol'n is

$$\{(x,y) = (480 - 9k, -360 + 7k) : k \in \mathbb{Z}\}$$

$480 - 9k > 0 \Rightarrow k < \frac{480}{9} = 53\frac{1}{3} \Leftrightarrow k \leq 53.$

$-360 + 7k > 0 \Rightarrow k > \frac{360}{7} = 51.4285\ldots \Leftrightarrow k \geq 52$

So $k \in \{52, 53\}$

We get two solutions with $x, y \in \mathbb{N}$

$(480 - 9\cdot 52, -360 + 7\cdot 52) = (12, 4)$

and

$(480 - 9\cdot 53, -360 + 7\cdot 53) = (3, 11)$

Problem 4: Find all $n \in \mathbb{N}$ such that $12 \mid n$ and $n \mid 816$

$12 = 2^2 \cdot 3$

$816 = 2^4 \cdot 3 \cdot 17$

All divisors of 816 in $\mathbb{N}$ have the form

$2^{e_1} \cdot 3^{e_2} \cdot 17^{e_3}$, where $0 \leq e_1 \leq 4$,
$0 \leq e_2 \leq 1$
$0 \leq e_3 \leq 1$.

12 divides the divisor, if furthermore,

$2 \leq e_1$ and $1 \leq e_2$.

So, $e_1 \in \{2, 3, 4\}$, $e_2 = 1$, $e_3 \in \{0, 1\}$

There are thus 6 such natural numbers

$2^2 \cdot 3$, $2^2 \cdot 3 \cdot 17$, $2^3 \cdot 3$, $2^3 \cdot 3 \cdot 17$, $2^4 \cdot 3$, $2^4 \cdot 3 \cdot 17$.

Problem 6:

(a) gcd(222, 189) via the Extended Euclidean Alg

$222 x_i + 189 y_i = r_i$

x_i	y_i	r_i	q_i
1	0	222	
0	1	189	
1	−1	33	1
−5	6	24	5
6	−7	9	1
−17	20	6	2
23	−27	3	1
		0	

gcd(222, 189)

$$\boxed{222 \cdot (23) + 189(-27) = 3}$$

(b) Similar to (a)

Problem 7; Let $a, b, c \in \mathbb{Z}$.
If $a | c$ and $b | c$, then $\text{lcm}(a,b) | c$.

Proof;

Method 1: (without the Fundamental Theorem of Arithmetic)

Write $c = q \cdot \text{lcm}(a,b) + r$, with
$0 \le r < \text{lcm}(a,b)$.

We need to prove that $r = 0$. The proof is by contradiction. Assume $r > 0$.
The natural numbers $r = c - q\,\text{lcm}(a,b)$ is a linear combination of c and $\text{lcm}(a,b)$ and both a and b divide c and $\text{lcm}(a,b)$. Hence, r is a common multiple, $r \in \mathbb{N}$, and $r < \text{lcm}(a,b)$. This contradicts the minimality of $\text{lcm}(a,b)$. Q.E.D.

Method 2; Let $c = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of c with $p_i \neq p_j$ if $i \neq j$ and $e_i \in \mathbb{N}$ for all i, Then
$a = p_1^{a_1} \cdots p_r^{a_r}$ with $0 \le a_i \le e_i$ and
$b = p_1^{b_1} \cdots p_r^{b_r}$ " $0 \le b_i \le e_i$ and
$\text{lcm}(a,b) = p_1^{\max\{a_1, b_1\}} \cdots p_r^{\max\{a_r, b_r\}}$, by Prop 6.2.4.
Now, $0 \le \max\{a_j, b_j\} \le e_j$ for all j, since both a_j and b_j satisfy these inequalities. Hence $\text{lcm}(a,b)$ divides c, by Prop 6.2.1. Q.E.D

Problem 8: Similar to Problem 6 (a)

Problem 9: Let $n \in \mathbb{N}$ and $k \mid n$. How many element belong to the set

$$S := \{ d \in \mathbb{N} : d \mid n \text{ and } k \mid d \} \ ?$$

Answer: If $n = 1$ then $k = \pm 1$ and $S = \{1\}$. Assume $n \geq 2$. Let $n = p_1^{e_1} \cdots p_t^{e_t}$ be the prime factorization of n with $0 < e_i$ and $p_i \neq p_j$, for $i \neq j$. Then

$$k = p_1^{k_1} \cdots p_t^{k_t}, \text{ with}$$

$0 \leq k_j \leq e_j$; $k_j \in \mathbb{Z}$.

So $S = \{ d = p_1^{d_1} \cdots p_t^{d_t} : k_j \leq d_j \leq e_j ; \ 1 \leq j \leq t \text{ and } e_j \in \mathbb{Z} \}$

The set S consists of

$$(e_1 - k_1 + 1)(e_2 - k_2 + 1) \cdots (e_t - k_t + 1)$$

elements.

Problem 10: Not included in the material

Problem 11: Similar to previous problems

Problem 12:

Let a, b, q, r be integers, such that $a = bq + r$. Prove that $\gcd(a,b) = \gcd(b,r)$.

Proof: This is Lemma 4.2.2 in the text, proven on page 159. Another proof is provided below. It suffices to prove that the sets of common divisors are equal

$$\underbrace{\{d \in \mathbb{N} : d \mid a \text{ and } d \mid b\}}_{= S_1}$$

$$= \underbrace{\{d \in \mathbb{N} : d \mid b \text{ and } d \mid r\}}_{= S_2}.$$

If $d \in S_1$ then d divides every linear combination of a and b with integer coefficients, so in particular it divides $r = 1 \cdot a + (-q) \cdot b$. Hence $d \in S_2$.

If $d \in S_2$, then d divides every linear combination of b and r with integer coefficients, in particular it divides $a = q \cdot b + 1 \cdot r$. Hence, $d \in S_1$. Thus, $S_1 = S_2$.

Q.E.D