Section 9.1

2) a) $42 = 1 \cdot 30 + 12$. $30 = 2 \cdot 12 + 6$. $12 = 2 \cdot 6 + 0$. $gcd(42, 30) = 6$.

b) $90 = 2 \cdot 39 + 12$. $39 = 3 \cdot 12 + 3$. $12 = 4 \cdot 3 + 0$. $gcd(90, 39) = 3$.

c) $153 = 1 \cdot 143 + 10$. $143 = 14 \cdot 10 + 3$. $10 = 3 \cdot 3 + 1$. $3 = 3 \cdot 1 + 0$. $gcd(143, 153) = 1$.

3) a) $6 = 30 - 2 \cdot 12 = 30 - 2(42 - 30) = 3(30) - 2(42)$.

b) $3 = 39 - 3 \cdot 12 = 39 - 3(90 - 2 \cdot 39) = 7(39) - 3(90)$.

c) $1 = 10 - 3 \cdot 3 = 10 - 3(143 - 14 \cdot 10) = 43(10) - 3(143) = 43(153 - 143) - 3(143) = 43(153) - 46(143)$.

4) a) In $\mathbb{Z}_7$, $(3 + 5)(6 + 4) + 6 = (1)(3) + 6 = 3 + 6 = 2$

b) In $\mathbb{Z}_6$, $(2^4 \cdot 3^2) + (2^4 \cdot 5) = (4 \cdot 3) + (4 \cdot 5) = 0 + 2 = 2$.

5) a) $11x = 1$ implies $11x + 24y = 1$. We use the Euclidean Algorithm. $24 = 2 \cdot 11 + 2$. $11 = 5 \cdot 2 + 1$. So

$$1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) = 11(11) - 5(24)$$

We see $x = 11$.

b) $41x = 1$ implies $41x + 77y = 1$. We use the Euclidean Algorithm. $77 = 1 \cdot 41 + 36$. $41 = 1 \cdot 36 + 5$. $36 = 7 \cdot 5 + 1$. So

$$1 = 36 - 7 \cdot 5 = 8(36) - 7(41) = 8(77) - 15(41)$$

We see $x = -15$, which in $\mathbb{Z}_{77}$, is equivalent to 62.

8)

$$\begin{aligned} q_1 b + r_1 &= q_2 b + r_2 \\ (q_1 - q_2) b &= r_2 - r_1 \end{aligned}$$

Since $0 \leq r_1 \leq r_2 < b$, we see that $0 \leq r_2 - r_1 < b$. However, we have just seen that $r_2 - r_1$ is a multiple of b. This forces $r_2 - r_1 = 0$. So $r_1 = r_2$. Therefore, $(q_1 - q_2)b = 0$, so $q_1 = q_2$ as well.

9) $k \cdot a = 0$ in $\mathbb{Z}_n$ means that n divides $k \cdot a$. Since $g = gcd(n, a)$, g divides both n and a. Therefore, $k \cdot a = \frac{n}{g} \cdot a = \frac{n \cdot a}{g} = n \cdot \frac{a}{g}$, and $\frac{a}{g}$ is an integer. Thus, n divides $k \cdot a$ as desired. Now suppose that $a \cdot x = 1$ in $\mathbb{Z}_n$ for some x. Then in $\mathbb{Z}_n$

$$k = k \cdot (a \cdot x) = (k \cdot a) \cdot x = 0 \cdot x = 0.$$

But $0 < k < n$, so $k \neq 0$ in $\mathbb{Z}_n$. Contradiction. $a \cdot x = 1$ has no solution.

10) Let p be prime and a be an arbitrary positive integer. $gcd(p, a)$ is a divisor of p, and so is either 1 or p. If it is 1, we are done. If it is p, then since $gcd(p, a)$ is also a divisor of a, we see $p|a$.

11) $1 = gcd(a, c)$. So there exist integers x, y such that $ax + cy = 1$. Thus, $abx + cby = b$. Since $c|ab$, $cn = ab$ for some integer n, and so $b = cnx + cby = c(nx + by)$. Therefore, $c|b$.

12) Let a, b, and p be positive integers with p prime and $p|ab$. By Problem 10, either $p|a$ or $gcd(p, a) = 1$. By Problem 11, if $gcd(p, a) = 1$, then $p|b$. Therefore, either $p|a$ or $p|b$.

13) Suppose that n has two factorizations into primes. $p_1^{r_1} \cdots p_k^{r_k} = n = q_1^{s_1} \cdots q_l^{s_l}$, where $p_1, \ldots, p_k$ are distinct primes, $q_1, \ldots, q_l$ are distinct primes, and $r_1 \ldots, r_k, s_1, \ldots, s_l$ are positive integers. For all $1 \leq i \leq k$, p_i divides $n = q_1^{s_1} \cdots q_l^{s_l}$, and so by Problem 12, p_i must divide one of the factors q_j on the right-hand side. Therefore, since q_j is prime, $p_i = q_j$. Therefore, each p_i is one of the q_j's. Reversing the argument shows that each q_j is one of the p_i's. In other words, the list of p_i's and q_j's are the same. Therefore, $k = l$, and we can assume $p_1 = q_1$, $p_2 = q_2$, etc.

So $p_1^{r_1} \cdots p_k^{r_k} = n = p_1^{s_1} \cdots p_k^{s_k}$. We need to show that $r_i = s_i$ for each i. Suppose for contradiction, that $r_1 < s_1$. Then $p_2^{r_2} \cdots p_k^{r_k} = p_1^{s_1 - r_1} p_2^{s_2} \cdots p_k^{s_k}$. $s_1 - r_1 \geq 1$, so p_1 divides the right-hand side, but does not divide the left-hand side. Contradiction. Therefore, $r_1 = s_1$. Similarly, $r_i = s_i$ for each i. Thus, the factorization is unique.

Section 9.2

1) a) $3x^2 + 5$

b) $2x + 3$

c) $2x^2 + 4x$

d) $x + 3$

2a) $2x^3 + x^2 - 9 = (2x - 5)(x^2 + 3x) + (15x - 9)$.

3a) $x^3 + x^2 + 1 = (x)(x^2 + x + 1) + (x + 1)$.

4a) $2x^2 + 3x + 4 = (3x + 3)(3x + 5) + (3)$.

9) a) $\max(-\infty, n) = n$ makes sense because $-\infty$ should be smaller than any number. The notation of $-\infty + n = -\infty$ makes sense if you consider a generalization of the statement for continuous functions $\lim_{x \to c}(a(x) + b(x)) = \lim_{x \to c} a(x) + \lim_{x \to c} b(x)$. Indeed, if we say $\lim_{x \to -\infty}(x + n) = (\lim_{x \to -\infty} x) + n$, we arrive at the desired equation.

b) If $q(x) = 0$, then $p(x)q(x) = 0$ no matter what p is. therefore, $\deg(p(x)q(x)) = \deg(0) = -\infty$, and $\deg(p(x)) + \deg(q(x)) = \deg(p(x) + -\infty = -\infty$, so the statement holds.

c) If $q(x)$ is the zero polynomial, then $\deg(p(x) + q(x)) = \deg(p(x)$, and

$\max(\deg(p(x)), \deg(q(x))) = \max(\deg(p(x)), -\infty) = \deg(p(x))$. Similarly, we get equality if $p(x)$ is zero. Finally, we need to consider the case where neither p or q are identically 0. Let $n = \deg p(x)$ and $m = \deg q(x)$.

$$\begin{aligned} p(x) &= a_n x^n + \ldots + a_0 \\ q(x) &= b_m x^m + \ldots + b_0 \end{aligned}$$

where a_n and b_n are nonzero. If $n > m$, then $a_n x^n$ is the leading term in $p(x) + q(x)$. Therefore, $\deg(p(x) + q(x)) = n = \max(n, m) = \max(\deg(p(x)), \deg(q(x)))$. Similarly, if $m > n$, then $\deg(p(x) + q(x)) = m = \max(\deg(p(x)), \deg(q(x)))$. Finally, if $m = n$, then the leading term of $p(x) + q(x)$ is $(a_n + b_n)x^n$ unless $a_n + b_n = 0$. If this is the case, then the degree can only decrease. Therefore, $\deg(p(x) + q(x)) \leq n = \max(\deg(p(x)), \deg(q(x)))$.