# *An Introduction to Abstract Algebra with Notes to the Future Teacher Complete Solutions*

## *Chapter 1*

### Section 1.1

1.

i. The answer is yes because any nonempty set of positive integers has a smallest member by the Well-Ordering Principle. The smallest member is 1 because we can write 1 as $1 = 139 \cdot 397 - 102 \cdot 541$.

ii. No. If $\frac{m}{n}$ is in the set, then $\frac{m}{2n}$ is also in the set. So there is no smallest member. The Well-Ordering Principle does not apply because the set in question is not a subset of the integers.

2. Let $P(n)$ be the statement that $1 + 3 + \ldots + (2n - 1) = n^2$. Then $P(1)$ is the statement that $1 = 1^2$, which is true. Now suppose that $P(n)$ is true. We prove that $P(n + 1)$ is true, namely, that $1 + 3 + \ldots + (2n - 1) + (2n + 1) = (n + 1).^2$ By our induction hypothesis, we can substitute $n^2$ for $1 + 3 + \ldots + (2n - 1)$. So we are left to prove that $n^2 + (2n + 1) = (n + 1)^2$, which is clearly true.

3. Let $n$ =1. Then $\frac{1-r^{n+1}}{1-r} = \frac{1-r^2}{1-r} = \frac{(1-r)(1+r)}{1-r} = (1+r)$ since $r \neq 1$. Assume $1 + r + r^2 + \ldots + r^n = \frac{1-r^{n+1}}{1-r}$. Then $1 + r + r^2 + \ldots + r^n + r^{n+1} = \frac{1-r^{n+1}}{1-r} + r^{n+1} = \frac{1-r^{n+1}}{1-r} + \frac{(1-r)r^{n+1}}{1-r} = \frac{1-r^{n+1}}{1-r} + \frac{r^{n+1}-r^{n+2}}{1-r} = \frac{1-r^{n+2}}{1-r}$.

4. Let $n = 1$. Then $n^3 + 2n = 3$, which is a multiple of 3. Assume $n^3 + 2n$ is a multiple of 3. We must show that $(n + 1)^3 + 2(n + 1)$ is a multiple of 3. Now $(n + 1)^3 + 2(n + 1) = n^3 + 3n^2 + 3n + 1 + 2n + 2$, which equals $(n^3 + 2n) + 3n^2 + 3n + 3$. Since $(n^3 + 2n)$ is a multiple of three, and $3n^2 + 3n + 3 = 3(n^2 + n + 1)$, $(n + 1)^3 + 2(n + 1)$ is a multiple of 3.

5. If there is one person in the room, there are 0 handshakes. Assume that if $n$ people are in the room, there are $\frac{n(n-1)}{2}$ handshakes. If an $(n + 1)^{th}$ person enters the room then $n$ more handshakes will occur, making the total $\frac{n(n-1)}{2} + n$. Now $\frac{n(n-1)}{2} + n = \frac{n(n-1)}{2} + \frac{2n}{2} = \frac{n^2-n}{2} + \frac{2n}{2} = \frac{n^2+n}{2} = \frac{n(n+1)}{2}$.

6. Proof by induction:

   Base Case: A tree consisting of a single node has one node, which is an odd number of nodes. Assume that a binary tree with fewer then $n$ nodes has an odd number of nodes. Let $T$ be a tree with $n$ nodes where $n > 1$ so that $T$ has a root with two offspring. Below the root node there are two trees, each with fewer than $n$ nodes. By induction, each of these trees has an odd number of nodes. So the number of nodes in the two sub trees combined is even. The additional root makes the number of nodes in the entire tree odd.

7. Reflexivity: For all pairs $(x, y)$, $0 = 2(x - x) = (y - y)$. So $(x, y)R(x, y)$.

   Symmetry: Assume $(x, y)\ R\ (s, t)$. Then $2(x - s) = (y - t)$. So $2(s - x) = (t - y)$ and $(s, t)R(x, y)$.

   Transitivity: Let $(x, y)\ R\ (s, t)$ and $(s, t)\ R\ (u, v)$. Then $2(x - s) = (y - t)$ and $2(s - u) = (t - v)$. Adding left and right sides, we get $2(x - u) = (y - v)$. Thus $(x, y)\ R\ (u, v)$.

   The equivalence class $[(1, 1)]$ consists of all points on the line $(y - 1) = 2(x - 1)$.

8. Suppose that $(x, y)R(s, t)$ and that $(u, v)R(w, z)$. To show that $[(x, y)] + [(u, v)] = [(s, t)] + [(w, z)]$, we must show that $(xv + yu, yv)\ R\ (sz + tw, tz)$. So we need to show that $(xv + yu)tz = yv(sz + tw)$ or, equivalently, that $xvtz + yutz = szyv + twyv$. From our assumptions, we can substitute $ys$ for $xt$ and $vw$ for $uz$ in left side of latter equation to obtain equality.

9. Reflexivity: $x\ Rx$ because $x$ is in the same member of $C$ as itself. Symmetry: If $xRy$, then $yRx$ since $y$ and $x$ are in the same member of $C$. Transitivity: If $xRy$ and $yRz$, then $x$ and $y$ are in the same set in $C$ and also $y$ and $z$ are in the same set in $C$. Since $y$ is in exactly one subset of $C$, $x$ and $z$ must be in the same subset. Therefore, $xRz$.

10. Let $\Sigma$ be the set of integers greater than $n_0$. Let $T$ be the subset $\Sigma$ of numbers **not** included in $S$. Assume that $T$ is not the empty set. The Well-Ordering Principle tells us that if $T$ is not empty, then $T$ has a smallest member, say $x$. Note that $x \neq n_0$ by the definition of $T$. Now if $x$ is the smallest natural number in $T$, then $x - 1$ is in $S$. But if $(x - 1) \in S$, then assumption ii insures that $(x - 1) + 1 = x$ is a member of $S$, contradicting our assumption that $x \notin S$. Thus $T$ must be empty and the set of integers greater than $n_0$ is therefore contained in $S$.

11. Let $P(n)$ be the statement, "If $S \subseteq \boldsymbol{N}$ contains any integer that is less than or equal to $n$, then $S$ has a smallest member." By proving that $P(n)$ is true for all $n$, we prove that every non-empty set of natural numbers has a least element, which is the Well-Ordering Principle. Here's the proof by induction: $P(1)$ is true because if a set contains the natural number 1, its smallest member is 1. Assume that $P(n)$ is true for the integer $n$. Let $S$ be a set that contains the integer $n + 1$. If $S$ contains no integer less than $n + 1$, then $n + 1$ is its smallest member. If $S$ does contain an integer less than $n + 1$, then it certainly contains an integer that is less than or equal to $n$. By the induction hypothesis, $S$ has a least member.

12. i. Let $e > 0$. By our assumption there is a natural number $n$ such that $n > \frac{1}{e}$. Taking reciprocals, we have $0 < \frac{1}{n} < e$.

ii. Let $e = y - x$. From part i we can find $n$ such that $\frac{1}{n} < e$. By the premise of the problem, there is an integer $m_0 > 0$ such that $m_0 > ny$ or, equivalently, $\frac{m_0}{n} > y$.

Let S be the set of integers $\{m : \frac{m}{n} > y\}$. Since $m_0 \in S$, $S$ is not empty. Since $y > 0$, every $m \in S$ is positive. Thus well ordering applies to $S$, and there is a smallest $q$ in $S$ such that $\frac{q}{n} > y$. So $\frac{q-1}{n}$ is less than $y$. We now show that $x < \frac{q-1}{n} < y$. Since $\frac{1}{n} < e$, we have $x < y - \frac{1}{n} < \frac{q-1}{n} < y$. Thus $\frac{q-1}{n}$ is a rational number between $x$ and $y$.

iii. If $x < 0$, let $q$ be any rational number greater than $|x|$. Let $r$ be a rational number between the positive numbers $x + q$ and $y + q$. Then $r - q$ is a rational number between $x$ and $y$.

**1.1 To the Teacher Tasks:**

1. The result of computing $\frac{x}{y} \div \frac{p}{q}$ must be a number $\frac{m}{n}$ such that $\frac{m}{n} \cdot \frac{p}{q} = \frac{x}{y}$. If we let $m = xq$ and $n = yp$, we get the correct result: $\frac{xq}{yp} \cdot \frac{p}{q} = \frac{x}{y}$. Of course, now we should back up and explain why the process of multiplying fractions by multiplying numerators and denominators is reasonable. The job of the teacher is to make this process both comprehensible and routine.

2.

| 1 | 1 + 3 | 1 + 3 + 5 | 1 + 3 + 5 + 7 |
|---|---|---|---|
| * | * *<br>* * | * * *<br>* * *<br>* * * | * * * *<br>* * * *<br>* * * *<br>* * * * |

## Section 1.2

1. Adding $-a$ to both sides, we obtain $-a + (a + b) = -a + (a + c)$. By the associative law, this is equivalent to $(-a + a) + b = (-a + a) + c$. Since $-a$ and $a$ are additive inverses we have $0 + b = 0 + c$. Since 0 is the additive identity, we obtain $b = c$.

2. First note that $0 = 1 + (-1)$. Thus, by Proposition 1, we have $0 = a(1 + (-1))$. Distributing, we obtain $0 = a + (-1)a$. By adding $-a$ to both sides we obtain $-a = 0 + (-1)a$ and so $-a = (-1)a$ .

3. First note that $-(-a) + (-a) = 0$. Adding $a$ to both sides we have
$(-(-a) + (-a)) + a = 0 + a = a$.
By associativity, we have $-(-a) + ((-a)+ a) = a$ and so $-(-a) + 0 = a$. Thus $-(-a) = a$

4. From Proposition 1, we know $(a + (-a))b = 0$. Distributing, we have $ab + (-a)b = 0$. Adding $-ab$ to both sides, we have $(-ab + ab) + (-a)b = -ab + 0$. Thus $0 + (-a)b = -ab$ or $(-a)b = -ab$

5. Assume that $ab = ac$ and that $a \neq 0$. By subtracting $ac$ from both sides, we obtain $ab - ac = 0$. By distribution, we have $a(b - c) = 0$. Since $a \neq 0$, $b - c = 0$. Adding $c$ to both sides, we have $b = c$. Here we need the fact that for integers, if $ab = 0$, either $a$ or $b$ (or both) must be 0.

6. Since $a$ divides $b$ and $a$ divides $c$ we can find integers $q$ and $p$ such that $b = aq$ and $c = ap$. So $(mb + nc) = (maq + nap) = a(mq + np)$. Thus $a \mid (mb + nc)$.

7. i. $335 = 19 \cdot 17 + 12$
ii. $-335 = (-20) \cdot 17 + 5$
iii. $21 = 1 \cdot 13 + 8$
iv. $13 = 1 \cdot 8 + 5$

8. Let $a \mid b$ and $c \mid d$. Then there exist integers $p$ and $q$ such that $b = pa$ and $d = cq$. We can multiply to get $acpq = bd$. So $bd$ is a multiple of $ac$. Thus $ac$ divides $bd$.

9. If $a = qb + r$, then $-a = (-q - 1)\, b + (b - r)$. (Note that $0 \leq (b - r) < b$.)

10. The integers $n$, $n$ +1, and $n$ +2 are three consecutive integers. So one of them is a multiple of three. So the product is a multiple of 3. Note, this can also be proved by induction.

11. Proof by Induction:
Base Case: Let $n = 0$. Then we have $2^{n+1} + 3^{3n+1} = 2 + 3 = 5$ and 5 certainly divides 5.
Assume that 5 divides $2^{n+1} + 3^{3n+1}$ so that there is an integer $q$ such that $5q = 2^{n+1} + 3^{3n+1}$.
Now consider $2^{n+2} + 3^{3n+4}$. Note that $2^{n+2} + 3^{3n+4} = 2 \cdot 2^{n+1} + 27 \cdot 3^{3n+1} = 2 \cdot 2^{n+1} + 2 \cdot 3^{3n+1} + 25 \cdot 3^{3n+1}$. This equals $2(2^{n+1} + 3^{3n+1}) + 25 \cdot 3^{3n+1} = 2(5q) + 5 \cdot 5 \cdot 3^{3n+1} = 5(2q + 5 \cdot 3^{3n+1})$. Thus 5 divides $2^{n+1} + 3^{3n+1}$, which proves that 5 divides $2^{n+1} + 3^{3n+1}$ for all $n \geq 0$.

**1.2 To the Teacher Tasks:**

1. $42321 = 104 \cdot 341 + 202$ in base five. In base 12, we let ten = T, and eleven = E. Then $42321 = 130 \cdot 341 + 1E1$.

## Section 1.3

1. i. 2; ii. 17; iii. 1; iv. 1

2.
   i. Any integer $x$ that divides both $m$ and $n$ divides both $-m$ and $-n$ and conversely. Thus the set of common divisors of $m$ and $n$ is identical to the set of common divisors of $-m$ and $-n$.
   ii. Since $|n|$ is a divisor of $n$, and it is the $\gcd(n, n)$ since no number larger than $|n|$ can divide $n$.
   iii. Since 1 divides any integer $n$, and no number greater than 1 divides 1, $\gcd(n, 1) = 1$.

3. By Theorem 1 we know that $am + bn = \gcd(a, b)$. If $x$ divides both $a$ and $b$, it divides both summands on the left side and thus it divides their sum.

4. Since $\gcd(a, c) = 1$, we can find integer $m$ and $n$ such that $1 = ma + nc$. Multplying through by $b$, we have $b = mab + ncb$. Now $ac$ divides $mab$ because $c$ divides $b$. Also $ac$ divides $ncb$ because $a$ divides $b$. Thus $ac$ divides the sum $b = mab + ncb$.

5. By Theorem 1, we can find integers s, $t$, $p$ and $q$ such that $1 = sx + tm$ and and $1 = py + qm$. Then $1 = spxy + (pyt + tqm + sxq)m$. Again by Theorem 1, $\gcd(xy, m) = 1$.

6. Since $a$ divides $a$ and since $a$ divides $b$, we know that $a$ is a common divisor of $a$ and $b$. It is the greatest common divisor since no number larger than $a$ divides $a$.

7. i. $23 = 1 \cdot 13 + 10$
   $13 = 1 \cdot 10 + 3$
   $10 = 3 \cdot 3 + \mathbf{1}$

   ii. $1234 = 10 \cdot 123 + 4$
   $123 = 30 \cdot 4 + 3$
   $4 = 1 \cdot 3 + \mathbf{1}$

   iii. $442 = 1 \cdot 289 + 153$
   $289 = 1 \cdot 153 + 136$
   $153 = 1 \cdot 136 + \mathbf{17}$
   $136 = 8 \cdot 17 + 0$

8. i. 102102
   ii. 3525
   iii. 39617

9. First note that if $n$ is odd, both $3n$ and $3n + 2$ are odd numbers. The first step of Euclid's Algorithm, applied to $3n + 2$ and $3n$ is as follows.
   $3n + 2 = 1 \cdot 3n + 2$.
   Thus $\gcd(3n + 2, 3n)$ is either 2 or 1. But it cannot be 2 since both $3n + 2$ and $3n$ are odd.

10. i. No solutions
    ii. $x = -6 + 5 \cdot t$
    $y = 9 - 7 \cdot t$
    iii. $x = -8 + 19t$
    $y = 20 - 47 \cdot t$

11. $x = 5 \cdot t$ for any positive integer $t$
    $y = 18 \cdot t - 3$

12.
Let $x$ denote the number of cocks, $y$ the number of hens and $z$ the number of groups of 3 chicks. Then $x + y + 3z = 100$ and $5x + 3y + z = 100$. Substitute $100 - 5x - 3y$ for $z$ in the first expression to obtain the Diophantine equation $7x + 4y = 100$. Its solutions are $x = -100 + 4t$ and $y = 200 - 7t$. Substitute the solutions for $x$ and $y$ into$100 - 5x - 3y = z$ to find that $z = t$. Its only positive

solutions are for $25 \le t \le 28$. So $(x, y, 3z)$ can equal (0, 25, 75) or (4, 78, 26) or (8, 11, 81) or (12, 4, 84).

13. i. $q_2 = 1$, $q_3 = 1$ and $q_4 = 3$. Thus $s_4 = 4$ and $t_4 = -7$. The sum $4 \cdot 23 - 7 \cdot 13 = 1$.
ii. $q_2 = 10$, $q_3 = 30$ and $q_4 = 1$. Thus $s_4 = 31$ and $t_4 = -311$. The sum $31 \cdot 1234 - 311 \cdot 123 = 1$.
iii. $q_2 = 1$, $q_3 = 1$ and $q_4 = 1$. Thus $s_4 = 2$ and $t_4 = -3$. The sum $2 \cdot 442 - 3 \cdot 289 = 17$.

**1.3 To the Teacher**

1. i. $\frac{1}{6}$; ii. $\frac{1}{24}$

Answer for 2.and 3. :

Suppose that $a = s/t$ and $b = u/v$ are positive rational numbers expressed in lowest terms and that $c = \text{lcm}(t, v)$. Then we can find integers $m$ and $n$ such that $a = m/c$ and $b = n/c$. As in the Division Algorithm, we can express $a$ uniquely as $m/c = qn/c + r/c$ where $q$ is an *integer*, $m = qn + r$, and $0 \le r < n$. Thus the number steps needed to carry out Euclid's Algorithm on $a$ and $b$ are exactly as many as needed for $m$ and $n$. Thus the Algorithm halts. Iterating, we see that the algorithm halts when $r = \gcd(m, n)$ and the remainder is $\gcd(m, n)/r$. Geometrically, we can think of lengths $a$ and $b$ as being multiples of a unit length $1/c$. Euclid's Algorithm finds the largest integer multiple of 1 that divides both $m$ and $m$. So Euclid's Algorithm applied $a$ and $b$ finds the largest integer multiple of $1/c$ of which both $m/c$ and $n/c$ are integer multiples.

## Section 1.4

1. $12347983 = 281 \cdot 43943$ and both factors are prime numbers.

2. i. Let $n_i$ be the minimum of $m_i$ and $k_i$. Then $\gcd(a, b) = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_n^{n_n}$
ii. $2^2 3^2 7^1$

3. i. Let $n_i$ be the maximum of $m_i$ and $k_i$. Then $\text{lcm}(a, b) = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_n^{n_n}$
ii. $2^5 3^5 5^1 7^2 11^2 13^3$

4. Every prime above 2 is odd. So if a prime is of the form $3m + 1$ then $m$ must be an even number. If $m$ is odd, then $3m$ is odd so $3m + 1$ is even and hence not prime. If $m$ is even, $m = 2 \cdot n$ for some integer $n$. Thus $3m + 1 = 3 \cdot 2 \cdot n + 1$ which is in the form $6n + 1$.

5. i. Let $n$ be a composite number and let $p$ be a prime that divides $n$ and let $q$ be another prime that divides $n$. Suppose that $p > \sqrt{n}$ and $q > \sqrt{n}$. Then $p \cdot q > \sqrt{n} \cdot \sqrt{n} = n$ so $p \cdot q > n$ which is a contradiction.

ii. 541 is indeed prime.

6. The first multiple of $n / 2$ is $n$. So for $p > n/2$ the multiples of $p$ will be outside of the range of numbers that we are searching.

7. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 + 1 = 200560490131$

8. Proof of Corollary 5. Suppose that $x$ is a rational number and that $x = m/n$. Let $d = \gcd(m, n)$ and $m = ds$ and $n = dt$ for some integers $s$ and $t$. By Proposition 3 of Section 1.3, $\gcd(s, t) = 1$. Note that $m/n = s/t$ because $mt = dst = dts = ns$.

9.

| | |
|---|---|
| 2 = 1 + 1 | 14 = 13 + 1 |
| 4 = 3 + 1 | 16 = 13 + 3 |
| 6 = 3 + 3 | 18 = 17 + 1 |
| 8 = 5 + 3 | 20 = 19 + 1 |
| 10 = 7 + 3 | 22 = 19 + 3 |
| 12 = 11 + 1 | 24 = 19 + 5 |

10. Let $p(i)$ denote the $i$th prime. Since $p(1) = 2$ and $2 \le 2^{2^{1-1}}$, the statement is true for $n = 1$. Suppose that $p(k) \le 2^{2^{k-1}}$ for $1 \le k \le n$. Then $1 + p(1)p(2)\cdots p(n) \le 1 + 2^{2^0}2^{2^1}\ldots 2^{2^{n-1}}$. Summing the exponents with the geometric formula, we have $1 + p(1)p(2)\cdots p(n) \le 1 + 2^{2^n - 1}$ and we know that $1 + 2^{2^n - 1} \le 2^{2^n}$. By the argument of Theorem 1, there must a prime between $1 + p(1)p(2)\cdots p(n)$ and $p(n)$. Thus $p(n + 1) \le 2^{2^n}$.

11. Let $p$ be any prime number. Since $p$ is prime the only factors of $p$ are 1 and itself. Suppose that $\sqrt{p}$ is rational. Then $\sqrt{p} = \frac{a}{b}$ where $a$ and $b$ are relatively prime non-zero integers, and $\left(\frac{a^2}{b^2}\right) = p$ so $a^2 = p \cdot b^2$. Since $p$ divides the right side of the equation it must also divide the left-hand side of the equation, and since $p$ is a prime it must divide $a$ (Euclid's Lemma) so we can rewrite $a$ as $p \cdot n$ which gives us the equation $p^2 \cdot n^2 = p \cdot b^2$. Dividing both sides by $p$ we get $p \cdot n^2 = b^2$ and so, by the same argument, $p$ must divide $b$. Thus $a$ and $b$ are not relatively prime, which is a contradiction.

**1.4 To the Teacher Tasks**

Challenge 1: 419,431,461

Challenge 2: [3, 197], [7, 193], [19, 181], [37, 163], [43, 157], [61, 139], [73, 127], [97, 103]

## Section 1.5

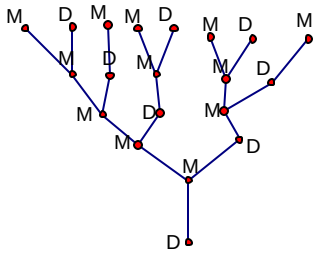
**Task 1.**

a. (In this problem, our indexing will be shifted.) Let $S_i$ be the number of ways to express $i$ as the sum of 1's and 2's . If $i = 1$, there is one way and so $S_1 = 0$ and if $i = 2$, there are2 ways, namely 2 = 1+1 and 2 = 2, so that $S_2 = 2$. Now if $i > 1$, any expression of $i$ as such a sum either terminates in 1 or 2 and the preceding summands sum to $i - 1$ and $i - 2$ respectively. The number of ways for the preceding summands to be expressed is $S_{i-1}$ and $S_{i-2}$ respectively. Thus $S_i = S_{i-1} + S_{i-2}$.

b. (In this problem, our indexing will be shifted.) Let $E_i$ be the number of ways the elf can jump $i$ steps. Then $E_0 = 1$ since there is exactly one way to jump no steps: Don't jump. There is exactly one way to jump to step 1 and so $E_1 = 1$. Now if the elf in on step $n$, he was previously either on step $n - 2$ or on step $n - 1$. There are $E_{i-2}$ and $E_{i-1}$ ways respectively to get to steps $n - 2$ or $n - 1$. Thus $E_i = E_{i-2} + E_{i-1}$.

c. (In this problem, our indexing will be shifted.) In the diagram below D stands for drone (or Dad) and M stands for mother. When $n = 0$, the number of grandmothers is 1. (She is seen two levels up from the root.) The mothers at any level $i$ are either mother to a female (M) at

level $i-1$ or a male (D) at level $i-1$ because every bee has a mother. The males at level $i-1$ are, in turn, in one-to-one correspondence with the mothers at level $i-2$ because every female has a father. Thus the number of mothers at level $i$ is the sum of the number of mothers at level $i-1$ and the number of mothers at level $i-2$.




**Lemma 1**.
***Proof.*** Suppose that $b = nc$. If $d|a$ and $d|\ c$, then $d|(a + nc)$. Conversely, if $d|(a + nc)$ and $d|\ c$, then $d|((a + nc) - nc)$.

**Proposition 3.**
***Proof.*** Since $F_0 = 0$, the proposition is true for $n = 0$. Assume that for all $0 \le i < n$, that $F_{m+i} = F_{m-1}F_i + F_mF_{i+1}$. Then $F_{m+(n-1)} = F_{m-1}F_{n-1} + F_mF_n$ and $F_{m+(n-2)} = F_{m-1}F_{n-2} + F_mF_{n-1}$. Adding, $F_{m+n} = F_{m-1}(F_{n-1} + F_{n-2}) + F_m(F_n + F_{n-1})$.

**Proposition 4.**
***Proof.*** It is clearly true for $n = 1$. Assume that $F_{mk}$ is divisible by $F_m$. By Proposition 2, $F_{mk+m} = F_{mk-1}F_m + F_{mk}F_{m+1}$.

**Proposition 5.**
***Proof.*** By proposition 2, $F_{qn+r} = F_{qn-1}F_r + F_{qn}F_{r+1}$. By proposition 3, $F_n$ divides $F_{qn}$. By proposition 1, $F_{qn-1}$ and $F_{qn}$ are relatively prime. Thus any common divisor of $F_r$ and $F_n$ is a divisor of $F_{qn-1}F_r + F_{qn}F_{r+1}$. Any common divisor of $F_{qn-1}F_r + F_{qn}F_{r+1}$ and $F_n$ must divide $F_{qn-1}F_r$ since $F_n$ divides $F_{nq}$. Since $F_{qn-1}$ and $F_{qn}$ are relatively prime, $F_n$ and $F_{qn-1}$ are relatively prime. Thus any common divisor of $F_{qn-1}F_r$ and $F_n$ must divide $F_r$.

**Theorem 6**.
***Proof.*** We can iterate proposition 4, carrying out the division theorem on the subscripts on the $F_i$. As with Euclid's algorithm, we will terminate with $\gcd(F_m, F_n) = \gcd(F_d, F_0)$ where $d = \gcd(m, n)$. Since $F_0 = 0$, $\gcd(F_d, F_0) = F_d$. Thus $\gcd(F_m, F_n) = F_d = F_{\gcd(m,n)}$.

**Additional Identities:**

1. Use induction on $n$ and note:
$$(F_n)^2 - F_{n+1}F_{n-1} = (F_n)^2 - (F_n + F_{n-1})F_{n-1} =$$
$$F_n(F_n - F_{n-1}) - (F_{n-1})^2 = F_nF_{n-2} - (F_{n-1})^2.$$

2. If there are $k$ 2s, then the number of addends of $n$ is $n-k$. So the problem can be rephrased as, "How many ways can we place $k$ 2s in a string of $n-k$ 2s and 1's?" The answer is $\binom{n-k}{k}$. The sum results when we add all possible counts of 2s.

In Pascal's Triangle we find the identity in adding the numbers in the ascending diagonals. One such diagonal is highlighted. Another is underlined. A third is italicized.

1
1 1
1 **2** 1
**1** 3 *3* 1
1 *4* 6 4 1
*1* 5 10 10 5 1

## Section 1.6

1. i. First express the numbers with a common denominator: $\frac{1}{2} = \frac{3}{6}$ and $\frac{1}{3} = \frac{2}{6}$. Then $\frac{3}{6} = 1 \cdot \frac{2}{6} + \frac{1}{6}$ and $\frac{2}{6} = 2 \cdot \frac{1}{6} + 0$. So the common measure of $\frac{1}{2}$ and $\frac{1}{3}$ is $\frac{1}{6}$. This means that both $\frac{1}{2}$ and $\frac{1}{3}$ are **integer** multiples of $\frac{1}{6}$ and that $\frac{1}{6}$ is the largest such rational number.

ii. $\frac{3}{8} = \frac{9}{24}$ and $\frac{5}{6} = \frac{20}{24}$. Now $\frac{20}{24} = 2 \cdot \frac{9}{24} + \frac{2}{24}$ and $\frac{9}{24} = 4 \cdot \frac{2}{24} + \frac{1}{24}$. Thus $\frac{1}{24}$ is the largest common measure.

2. For two fractions *p/n* and *q*/*n* expressed over a common denominator *n*, the algorithm takes exactly as many steps as when it is applied to *p* and *q*.

3. i. {0; 1, 2, 3} = $\frac{7}{10}$ and {3; 1, 2, 1, 2, 1, 2} = $\frac{153}{41}$.

4. We get $\frac{1}{2}$, then $\frac{2}{3}$, then $\frac{3}{5}$. Continuing, we get the ratios of consecutive Fibonacci numbers.

5. i . {0; 2, 1, 5, 2}, ii. {2; 11}, iii. { 1; 4, 1, 1, 1, 2}

6. i. {3; 7, 7}, ii. {3; 7, 16,11}

7. {1;1, 1, 1, …}

8. The continued fraction approximation for *e* with 10 terms is {2; 1,2,1,1,4,1,1,6,1}. This evaluates to **2.71828**3582. With the same number of places, the calculator's approximation to *e* is **2.71828**1828.

9. For both i and ii, notice that $a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{(a_n - 1) + 1} = a_{n-1} + \frac{1}{(a_n - 1) + \frac{1}{1}}$.

## Section 1.7

1. No since 15 is divisible by 5.

2. The sequence of remainders is {0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7}.

3. $a^{12} = (a^2)^6$ and by Fermat's Theorem , $(a^2)^6 - 1$ is divisible by 7. Similarly, $(a^3)^4 - 1$ is divisible by 5. Since 5 and 7 are relatively prime, $a^{12} - 1$ is divisible by 35.

4. $3^{100} = (3^{25})^4$ which has a remainder 1 after division by 5 by Fermat. Thus the final digit of $3^{100}$ is either 1 or 6. Since $3^{100}$ is odd, the final digit is 1.

5. Since $91 = 13 \cdot 7$ and 91 divides $3^{90} - 1$, we cannot use Fermat's Theorem to test for primes because there are non-prime values of $p$ for which the conclusion holds for some values of $a$. But if there is any $a$ for which the result does not hold, we are guaranteed that $p$ is not prime.

6. $(a^q - 1)(a^q + 1) = a^{p-1} - 1$ which is divisible by $p$. By Euclid's Lemma, one of the factors must be divisible by $p$. By the Division Theorem, $(a^q + 1) = 1 \cdot (a^q - 1) + 2$. So the gcd of $(a^q - 1)$ and $(a^q + 1)$ can only be 1 or 2. Since $p$ is and odd prime greater than 2, it cannot divide both factors.

7. 63504

8. In $\sum_d c(d)$, each integer $x$ between 1 and $n$ is counted exactly once by $c(d)$ where $d = \gcd(x, n)$. Thus $\sum_d c(d) = n$. Let $d$ be a positive divisor of $n$. To see that $c(d) = \phi(n/d)$, first note that the multiples of $d$ that divide $n$ are of the form $i \cdot d$ for a subset of the values of $i$ such that $1 \le i \le \frac{n}{d}$. Of these values of $i$, $\gcd(i \cdot d, n) = d$ if and only if $\gcd(i, n) = 1$. Thus there are exactly $\phi(n/d)$ such values of $i$.

9. i. $\tau(2) = 2$ and $\sigma(2) = 3$; $\tau(10) = 4$ and $\sigma(10) = 18$; $\tau(28) = 6$ and $\sigma(28) = 56$.

   ii. The positive divisors of $n$ are all of the form $p_1^{x_1} p_2^{x_2} \ldots p_q^{x_q}$, where $0 \le x_i \le n_i$. Thus there are $n_i + 1$ possibilities for the exponent of $p_i$.

   iii. Proof by induction on the number $q$ of distinct prime factors of $n$. If $q = 1$, then $n = p^{n_1}$ for some prime $p$ and positive $n_1$. Its divisors are $1, p, \ldots, p^{n_1}$. Their sum is $\frac{1 - p^{n_1+1}}{1 - p}$. Now suppose the assertion holds for numbers that factor into powers of $q - 1$ distinct primes and assume that $n$ factors as $p_1^{n_1} p_2^{n_2} \ldots p_q^{n_q}$. By the induction hypothesis, the sum of the factors of the form $p_1^0 p_2^{i_2} \ldots p_q^{i_q} = \prod_{i=2}^{q} \frac{1 - p_i^{n_i+1}}{1 - p_i}$. Let $S$ be the set of all factors of the form $p_1^0 p_2^{i_2} \ldots p_q^{i_q}$. Then $\sigma(n) = \sum_{i=0}^{n_1} \sum_{a \in S} p_1^i a = \sum_{i=0}^{n_1} p_1^i \left( \sum_{a \in S} a \right) = \left( \frac{1 - p_1^{n_1+1}}{1 - p_1} \right) \left( \prod_{i=2}^{q} \frac{1 - p_i^{n_i+1}}{1 - p_i} \right) = \prod_{i=1}^{q} \frac{1 - p_i^{n_i+1}}{1 - p_i}$.

   iv. $\tau(n) = 72$; $\sigma(n) = 191319912000$

10. If $m$ and $n$ are relatively prime, then the prime factors of $mn$ are the disjoint union of the factors of $m$ and the factors of $n$.

11. Note that $(2^n - 1)$ and $(2^{n-1})$ are relatively prime. Since $(2^n - 1)$ is prime, $\sigma((2^n - 1)) = 2^n$. Also $\sigma(2^{n-1}) = 2^n - 1$. So $\sigma((2^n - 1)(2^{n-1})) = (2^n - 1)(2^n)$. The sum of the divisors strictly less than

$(2^n - 1)(2^{n-1})$ is $(2^n - 1)(2^n) - (2^n - 1)(2^{n-1}) = (2^n - 1)(2^{n-1})$. Thus if $(2^n - 1)$ is prime, $(2^n - 1)(2^{n-1})$ is a perfect number. The first four perfect numbers are 6, 28, 496, and 8128. Looking further:

191561942608236107294793378084303638130997321548169216

is a perfect number! (Let $n = 89$.)

12. Note that $1729 = 7 \cdot 13 \cdot 19$. Then $a^{37} - a = a((a^6)^6 - 1) = a((a^3)^{12} - 1) = a((a^2)^{18} - 1)$

## Section 1.8

**In The Classroom: Problem Solving**
Social Security Number: 381654729

## Section 1.9

1. $2^{35} - 1 = (2^7)^5 - 1 = (2^7 - 1)(2^{28} + 2^{21} + 2^{14} + 2^7 + 1)$. $2^7 - 1 = 127$ is a factor. Similarly we find that $2^5 - 1 = 31$ is a factor.

2. We need to find four primes of the form $2 \cdot 17k + 1$ that are less than the square root of $2^{17} - 1$. The required square root is less than 363. Starting with $k = 1$ we have the following numbers to check: 35, 69, 103, 137, 171, 205, 239, 273, 307, and 341. Checking for small factors we can remove 35, 69, 171, 205, 273, and 341 from the list. Thus the four primes are 103, 137, 239, and 307.

3. The first prime to check is $2 \cdot 2) + 1 = 47$. $(2^{23} - 1)/47 = 178481$.

4. For $n = 13$, the smallest $r$ is 12.
   For $n = 17$, the smallest $r$ is 8 and 8 divides $17 - 1 = 16$.
   For $n = 19$, the smallest $r$ is 18.

5. For $n = 5$, the smallest $r$ is 4.
   For $n = 7$, the smallest $r$ is 6.
   For $n = 11$, the smallest $r$ is 5 and 5 divides $11 - 1$.

6. Suppose that $p$ is odd. Then $2^{pq} + 1 = (2^q)^p + 1 = (2^q + 1)(2^{q(p-1)} - 2^{q(p-2)} + \ldots - 2^q + 1)$. Thus $2^q + 1$ is a factor. For example $2^2 + 1 = 5$ is a factor of $2^6 + 1 = 65$.

## Chapter 1 Highlights: Chapter Questions

3. i. $q = 0$, $r = 2$; ii. $q = 26$, $r = 21$; iii. $q = -27$, $r = 36$

4. i. $456 = 1 \cdot 234 + 222$; $234 = 1 \cdot 222 + 12$; $222 = 18 \cdot 12 + \mathbf{6}$; $12 = 2 \cdot 6 + 0$.

   ii. $589403 = 6 \cdot 93840 + 26363$; $93840 = 3 \cdot 26363 + 14751$; $26363 = 1 \cdot 14751 + 11612$;
   $14751 = 1 \cdot 11612 + 3139$; $11612 = 3 \cdot 3139 + 2195$;
   $3139 = 1 \cdot 2195 + 944$; $2195 = 2 \cdot 944 + 307$; $944 = 3 \cdot 307 + 23$; $307 = 13 \cdot 23 + 8$;
   $8 = 1 \cdot 7 + \mathbf{1}$; $7 = 1 \cdot 7 + 0$

   iii. The gcd of any two consecutive Fibonacci numbers is 1.

5. i. no solutions since gcd(30, 12) does not divide 27
ii. $12 = 12(-6 + t \cdot 17)31 + 12(11 - t \cdot 31)17$ for any integer $t \in \boldsymbol{Z}$.

6. With $p = 7$, we have $12^{7651} = 12^{6 \cdot 1275 + 1}$. By Fermat's Little Theorem, the remainder $12^{7651}$ after division by 7 is equal to the remainder of $12^1$ after division by 7. Thus the answer is 5.

7. 1123668000

8. i. 5952; ii. 130628; iii. 144;

10. Proof. Since $x$ divides $xs$ and $xs = yt$, $x$ divides $yt$. Since $\gcd(x, y) = 1$, $x$ divides $t$. (Euclid's Lemma). Similarly, $y$ divides $s$.

## *Chapter 2*_____

### Section 2.1

1. $[13]_9 = \{\ldots -14, -5, 4, 13, 22, 31, 40, \ldots\}$, $[3]_{10} = \{...-17, -7, 3, 13, 23, 33, 43, \ldots\}$, $[4]_{11} = \{\ldots -18, -7, 4, 15, 26, 37, 48, \ldots\}$

2. Since $m \mid (a - b)$, it follows that $m \mid k(a - b)$ for all $k$ in $\boldsymbol{Z}$.

3. Since $m \mid (a - b)$ and $m \mid (c - d)$, it follows that $m \mid ((a + c) - (b + d))$.

4. If $a \equiv b \bmod m$ and then the statement is true for $n = 1$. Assume that $a^{n-1} \equiv b^{n-1} \bmod m$. We can apply part iii of Theorem 2 to $a^{n-1} \equiv b^{n-1} \bmod m$ and $a \equiv b \bmod m$ to conclude that $a^n \equiv b^n \bmod m$

5. Since $103 \equiv 3 \bmod 5$, we can determine $103^{45} \equiv 3^{45} \bmod 5$. Since $3^4 \bmod 5 = 1$, we have $3^{45} \bmod 5 = (3^4)^{11}3^1 \bmod 5 = 3$.

6. We can see that $58 \bmod 11 = 3$ and a bit of experimenting reveals that $3^5 \bmod 11 = 1$. Thus $58^{29} \bmod 11 = 3^{29} \bmod 11 = (3^5)^5 3^4 \bmod 11 = 3^4 \bmod 11$. Now $3^4 = 81$ and $81 \bmod 11 = 4$.

7. The terminal digit of $a$ must be 1, 2, 3 or 4. Thus the terminal digit of $a^2$ must be 1, 4, 9, or 6. So $a^2 \bmod 5$ must be 1 or 4. With the same reasoning, $a^4 \bmod 5 = 1$.

8. We can state Euler's Theorem as follows. "If $a$ and $m$ are relatively prime, then $a^{j(m)} \equiv 1 \bmod m$." We can state Fermat's Little Theorem as, "If $p$ is prime, then for any integer $a$, $a^p \equiv a \bmod p$."

9. The solution sets are:
   i. empty
   ii. $[1]_8 \cup [3]_8 \cup [5]_8 \cup [7]_8$
   iii. empty
   iv. $[3]_5$
   v. $[6]_{11}$

10. The integer $x_0$ is a solution to $ax \equiv b \bmod m$ if and only if there exists a $q_0$ such that $x_0$ and $q_0$ satisfy the Diophantine equation $ax - qm = b$. In that case, all other values of $x$ are of the form $x = x_0 + \frac{im}{d}$ by Proposition 8 of Section 1.3.

11. The solution sets are:
    i. $[4]_{15} \cup [9]_{15} \cup [14]_{15}$
    ii. $[6]_{35} \cup [13]_{35} \cup [20]_{35} \cup [27]_{35} \cup [34]_{35}$
    iii. $[15]_{19}$

12. Since $rx \equiv rb \bmod m$, we can find an integer $q$ such that $rx - rb = qm$. Now divide both sides by $d = \gcd(r, m)$. Then $\frac{r}{d}(x-b) = \frac{m}{d}q$. Since $\frac{r}{d}$ and $\frac{m}{d}$ are relatively prime and since $\frac{m}{d}$ divides $\frac{r}{d}(x-b)$, $\frac{m}{d}$ must divide $(x-b)$.

13.
    i. $7x \equiv 5 \bmod 11$ ; An inverse of 7 is 8 since $56 \equiv 1 \bmod 11$. Thus $8 \cdot 5 \equiv 40 \bmod 11$ and $40 \equiv 7 \bmod 11$. So $x = [7]_{11}$
    ii. $8x \equiv 2 \bmod 6$ ; no inverse; $x = [1]_6$ and $x = [4]_6$
    iii. $5x \equiv 3 \bmod 12$; The inverse of 5 is 5 since $25 \equiv 1 \bmod 12$. Thus $25x \equiv 15 \bmod 12$ and $15 \equiv 3 \bmod 12$. Thus $x = [3]_{12}$

14.
i. The inverse of 31 is 12 mod 53 and the solution set is $[11]_{53}$
ii. The inverse of 23 is 27 mod 31 and the solution set is $[2]_{31}$

15. i. 4; ii. 1; iii. 2.

16.
i. ***Proof.*** $a^2 \equiv 1 \bmod p$ iff $p \mid (a^2 - 1)$. Now $p \mid (a^2 - 1)$ iff $p \mid (a-1)(a+1)$. By Euclid's lemma, $p \mid (a-1)(a+1)$ iff $p \mid (a-1)$ or $p \mid (a+1)$.
ii. ***Proof.*** The number of elements in the set $\{p-1, p-2, \ldots, 1\}$ is even. Of these numbers, only $p-1$ and 1 are their own inverses. So every other number has a distinct inverse in the list. So when we write out the product $(p-1)(p-2)\ldots 1 \bmod p$, we can replace each pair of inverses with 1 mod $p$. We are left with $(p-1)! \equiv (p-1) \bmod p$ or equivalently, $(p-1)! \equiv -1 \bmod p$.

17. $[206]_{210}$

18. $[535]_{1001}$

19. The number of coins is 3930.

20. Let $d = \gcd(m, n)$. We know that $x$ is a common solution to $x \equiv b \bmod m$ and $x \equiv a \bmod n$ if and only if $a - b = qm - pn$ for some integers $q$ and $p$. The Diophantine equation $a - b = qm - pn$ has a solution if and only if $a - b$ is divisible by $d$. Now suppose that $x$ and $y$ are both

simultaneous solutions to $x \equiv b \bmod m$ and $x \equiv a \bmod n$. Then we can find integers $t$ and $s$ such that $x - y = tm = sn$. Since $m/d$ and $n$ are relatively prime, $m/d$ divides $s$ by Euclid's Lemma. So $s = vm/d$ for some integer $v$. Thus $x - y = vmn/d$. Since $\text{lcm}(m, n) = mn/d$, we have that $x$ and $y$ are congruent modulo $\text{lcm}(m, n)$.

**2.1 To the Teacher Tasks**

1. $d_{12} = 7$
2. If an odd digit is changed by +3 and an even digit is changed by +1, the error will not be detected.

## Section 2.2

**Proposition A and Corollary 1:**
**Proof.** $10^n = 999\ldots9 + 1$, which is congruent to 1 mod 9. Thus $a10^n \equiv a \bmod 9$.

**Trick 1**: $x_n10^n + x_{n-1}10^{n-1} + \ldots + x_0 \equiv x_n + x_{n-1} + \ldots + x_0 \bmod 9$ by Corollary B.

**Trick 2**. The argument is the same as for Trick 1 because $10^n = 999\ldots9 + 1$ is congruent to 1 mod 3.

**Trick 3**: Apply hint.

**Trick 4**. First note that a number $x$ that ends in a zero is divisible by 7 if and only if the integer $\frac{x}{10}$ is divisible by 7 because the smallest multiple of 7 that ends in 0 is 70. (In "short" division, we would have to carry a 7 or a 0 to the last digit. The former is impossible and the later implies that $\frac{x}{10}$ is divisible by 7. ) Now suppose that $d$ is the last digit.

**Trick 5.** This trick is also based on Proposition A and Corollary B:
$(x_n + y_n)\, 10^n + (x_{n-1} + y_{n-1})\, 10^{n-1} + \ldots + (x_0 + y_0) \equiv (x_n + y_n) + (x_{n-1} + y_{n-1}) + \ldots + (x_0 + y_0) \bmod 9$.
The case for multiplication is similar.

**Additional tasks:**

1. The analogy to Proposition A in base 5 is that $5^n = 4..44 + 1$. The analogous test for division of $x$ by 4 is to test that the sum of its digits is divisible by 4. (All computations are carried out base 5.) We can generalize the test for divisibility by $m - 1$ in base $m$.

2. Just like 11 base 10, 6 has a remainder of 1 mod 5. So the trick is to test the alternating sum of digits.

3. This test will NOT detect all errors. For instance, it will not detect transposed digits in the answer

4. Interpret the hint with Proposition A and its corollary.

## Section 2.3

**Task 1.** $214^{43} \bmod 221 = 20$ T

$70^{43} \bmod 221 = 8$ H
$100^{43} \bmod 221 = 9$ I
$92^{43} \bmod 221 = 14$ N
$158^{43} \bmod 221 = 11$ K

**Task 2.** SEND _HELP (There's an extra symbol that we can interpret as a space.)

**Task 3.** 208 1 214 70 100 59 46 200 92

**Task 4.**

Encode: 7335 4585 6397 6741 2984 1 3197

Decoded: 7 15 27 8 15 13 5 or GO HOME

**Task 5.** $j$ = 903595073 Decoded: 7 15 20 3 8 1 or GOTCHA

**Task 6.** $M^{kj} = M^{1 + s(p-1)(q-1)/d} = M\,(M^{p-1})^{s(q-1)/d}$. By Fermat's Little Theorem, $M^{p-1} \equiv 1 \bmod p$ and so $M^{kj} \equiv M\,(M^{p-1})^{s(q-1)/d} \equiv M \bmod p$. Similarly, $M^{kj} \equiv M \bmod q$. Since $\gcd(p, q) = 1$, $M^{kj} \equiv M \bmod pq$. (Note: This assumes that the primes chosen are larger than the digits to be encoded. Otherwise, it works when $M$ and $n$ are relatively prime. )

## Section 2.4

1.

| $Z_3$, + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $Z_3$, * | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

| $Z_4$, + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\boldsymbol{Z_4}$, * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

2. Suppose that $x \in [a]_m$ and $y \in [b]_m$. Then $a \equiv x \bmod m$ and $b \equiv y \bmod m$. By Theorem 2 of Section 2.1, $ab \equiv xy \bmod m$. Therefore $[ab]_m = [xy]_m$.

3. i. 0; ii. 3; iii. 2; iv. 2

4. $[a]_m([b]_m + [c]_m) = [a]_m \cdot ([b + c]_m) = [a(b + c)]_m = [ab + ac]_m = [ab]_m + [ac]_m = [a]_m \cdot [b]_m + [a]_m \cdot [c]_m$

5. i. 4; ii. 3; iii. 4; iv. 10; v. 8; vi.{2, 5, 8, 11}

6. $m = 12$: The units are 1, 5, 7, 11. Their inverses are 1, 5, 7, 11 respectively.
$m = 9$: The units are 1, 2, 4, 5, 7, 8. Their inverses are 1, 5, 7, 2, 4, and 8 respectively.
$m = 10$: The units are 1, 3, 7, 9. Their inverses are 1, 7, 3, and 9 respectively.
$m = 11$: The units are 1 through 10. The inverses are (in order) {1, 6, 4, 3, 9, 2, 8, 7, 5, 10}.

7. Let $p$ be prime. Then for all $x$ such that $0 < x < p$, $\gcd(x, p) = 1$ and $ax \equiv 1 \bmod p$ has a solution.

8. The congruence $ax \equiv 1 \bmod m$ has a solution if and only if $\gcd(a, m) = 1$.

9. Suppose that $a$ be a nonzero element in $\boldsymbol{Z_m}$. Let $d = \gcd(a, m)$ and $y = m/d$. If $d > 1$, then $a$ is a zero divisor because $ay = 0$ in $\boldsymbol{Z_m}$ but $y \neq 0$. Conversely, if $d = 1$, and $ay \equiv 0 \bmod m$, then $m \mid y$. So $y = 0$ in $\boldsymbol{Z_m}$ and $a$ is not a zero divisor.

10. There are $j(m)$ units in $\boldsymbol{U_m}$.

| $\boldsymbol{U_{12}}$, * | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

| $\boldsymbol{U_8}$, * | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

11. No. For instance, in $\boldsymbol{Z_6}$, $2 \cdot 4 = 2 \cdot 1$ but, canceling the 2, $4 \neq 1$.

12. Let $m = 6$. Then $4 + 4 = 1 + 1$ but $4 \neq 1$.

13. Let $m = 9$. Then $4 + 4 + 4 = 1 + 1 + 1$ but $4 \neq 1$.

14. In $\boldsymbol{Z_7}$, 3 is such an element because $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. This can not be done for $\boldsymbol{Z_8}$ because each nonzero element squared is equal to 1. It cannot be done in $\boldsymbol{Z_{10}}$. In $\boldsymbol{Z_{11}}$, 2 works.

**2.4 To the Teacher Tasks**

1. For instance, $1 < 4$ but is $1 + 1 < 1 + 4$?
2. The symbol $\frac{1}{p}$ is used to denote a value of $x$ such that $x \cdot p = 1$. Just writing the symbol $\frac{1}{p}$ does not imply that you can find such a value of $x$. It is not immediately obvious that among all the numbers that you can express as non-repeating, non-terminating decimals, there is a number that satisfies the equation $x \cdot p = 1$. (A proof of existence is an exercise in analysis.)

## Section 2.5

1. iii. $(-a)(-b) + (-a)(b) = (-a)(-b + b) = (-a)0 = 0$. Since by part ii, $(-a)b = -(ab)$ we also have that $-(ab)$ is the additive inverse of both ($ab$) and (-$a$)(-$b$). Thus these two are equal since their additive inverses are unique.

   iv. $(-1)a = -(1a) = -a$ again applying part ii.

2. Suppose that 1 and $x$ are unities in the same ring. Then $1 = 1 \cdot x = x$.

3. Suppose that $a$ and $b$ are multiplicative inverses of $x$ in a ring $R$. Then $(ax)b = a(xb)$ by associativity. So $(ax)b = 1 \cdot b = b = a(xb) = a \cdot 1 = a$. Thus the two inverses are equal.

4. Let $d = \gcd(x, m)$. Let $y = m/d$. If $d \neq 1$, then $xy = 0$ in $\boldsymbol{Z_m}$ but $y \neq 0$. Thus $x$ is a zero divisor in $\boldsymbol{Z_m}$. Conversely, if $d = 1$ and $xy = 0$ in $\boldsymbol{Z_m}$, then $m$ divides $y$ so that $y = 0$ in $\boldsymbol{Z_m}$ and $x$ is not a zero divisor.

5. The symbol 2 has a multiplicative inverse in $\boldsymbol{Z_5}$ and in $\boldsymbol{Z_{15}}$ but not in $\boldsymbol{Z_4}$ or $\boldsymbol{Z_{20}}$. Thus 2 can be cancelled in $2x = 2y$ in $\boldsymbol{Z_5}$ and in $\boldsymbol{Z_{15}}$ but not in the others.

6. In $\mathbf{M}_{2\times 2}$, let $x = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $y = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Then $(x + y)^2 = x^2 + xy + yx + y^2 = \begin{bmatrix} 13 & 18 \\ 24 & 37 \end{bmatrix}$ but $x^2 + 2xy + y^2 = \begin{bmatrix} 12 & 17 \\ 24 & 38 \end{bmatrix}$. (In a non-commutative ring, the expansion of $(x + y)^n$ would have

$\binom{n}{i}$ monomials that contained exactly $i$ copies of $x$ and $n - i$ of $y$. However, each arrangement of a monomial would need to be counted individually because, for instance, we could not assume that $xxyxyxy = x^4y^2$. Thus $(x + y)^n$ would have $2^n$ distinct monomials in its expansion.

7. The units of $\boldsymbol{Z}_m$ are the elements that are relatively prime to $m$. If $\gcd(x, m) = 1$ then there are integers $u$ and $v$ such that $ux + vm = 1$. Thus $ux = 1 - vm$ and $ux = 1$ in $\boldsymbol{Z}_m$. So $x$ is a unit. If $\gcd(x,m) \neq 1$, then $x$ is a zero divisor and hence not a unit. (See Exercise 4.)

8. The units in $\boldsymbol{Q}[x]$ are the non-zero rational numbers. Each non-zero rational number has a multiplicative inverse. Since the symbol $x$ does not have a multiplicative inverse, no non-constant polynomial is a unit.

9. Let $p(x) = a_nx^n + \ldots..+a_0$ and $q(x) = b_kx^k + \ldots + b_0$ be two non-zero polynomials with coefficients in a ring $R$. Suppose that neither $a_n$ nor $b_k = 0$. Their product is $a_nb_kx^{n+k} + \ldots + a_0b_0$. If $R$ is an integral domain, $a_nb_k \neq 0$ and so the $p(x)q(x) \neq 0$. Thus $R[x]$ is an integral domain. Conversely, suppose $R$ is not an integral domain, and let $a$ and $b$ be zero divisors in $R$. Let $p(x) = a$ and $q(x) = b$. Then $p(x)q(x) = 0$ and $R[x]$ is not an integral domain.

10. If $R$ is a ring without unity, then clearly $R[x]$ is not a field because it has no unity element. If $R$ is a ring (or field) with unity, the polynomial $p(x) = x$ has no inverse.

11. In $\boldsymbol{Z}_5$, $x = 2$. In $\boldsymbol{Z}_7$, there is no solution.

12. $ad - cb \neq 0$.

13. The multiplicative inverse of a non-zero element $a + b\sqrt{5}$ is $\dfrac{a - b\sqrt{5}}{a^2 - 5b^2}$

14. To show that $\boldsymbol{Z}_3[i]$ is a field we need to show that every non-zero element has a multiplicative inverse. Consider $a + bi$ where $a$ and $b$ are elements of $\boldsymbol{Z}_3$ and are not both zero. Then $(a + bi)(a - bi) = a^2 + b^2$. The square of an element in $\boldsymbol{Z}_3$ is either 0 or 1. It can not be 2. The possible values of $a^2 + b^2$ are 1 or 2. If it is 1, then $a - bi$ is the multiplicative inverse. If the value of $a^2 + b^2$ is 2 then $2a - 2bi$ is the multiplicative inverse of $a + bi$. The multiplicative inverse of $2 + i$ is $2(2 - i) = 1 - 2i$. To solve $(2 + i)x = 1 + 2i$, multiply both sides by $1 - 2i$ so that $(1-2i)(2+i)x = x = (1-2i)(1+2i) = 1 + 1 = 2$.

15. No, because $(2 + i)(2 - i) = 4 + 1 = 0 \bmod 5$.

16. If $x^2 = x$, then $x^2 - x = 0$ or $x(x - 1) = 0$. In an integral domain, it must be the case that $x = 0$ or $x - 1 = 0$. Thus the only solutions are $x = 0$ and $x = 1$.

17. The sum of any polynomial with itself $p$ times results in the zero polynomial.

18. As per the hint, $T_x$ is injective since if $xy = xz$, we have $x(y - z) = 0$. Since $x \neq 0$, $y - z = 0$ or $y = z$. Since an injective map on a finite set must be surjective, we can find $z$ in $R$ such that $xz = 1$. Thus every nonzero element in $R$ is a unit and $R$ must be a field.

**2.5 To the Teacher Tasks**

2. If the mouse uses $n$ or more doors, then it must visit one of the $n$ stations more than once. It could find a trip with no repeated stations that uses fewer doors.
3. No! In figure 1, a mouse cannot get back to station 6 or to station 1.
4. Yes, if there is a loop like $2 \to 3 \to 4 \to 2$ which can be traversed any number of times.

5. Yes, if there are no such loops as $2 \to 3 \to 4 \to 2$, a mouse could never get back to where it started.
6. E.g. Power transmission lines.
7. The matrix $A^2$ would contain a 1 in position $i$-$j$ if there is at least one path between stations $i$ and $j$ using exactly 2 doors 0 otherwise. The matrix would summarize the existence of paths, but not count the number of paths.

## Section 2.6

1. $z + w = 3 - 2i$; , $zw = 5 - 5i$; $z/w = (-1/5 - 7i/5)$;
   $w^2 = 3 + 4i$; $z^3 = -26 + 18i$.
2. $z = 1 + i/3$.
3. Both are sides are equal to $(ac + ae - bd - bf) + (ad + af + bc + be)\, i$

4. $\frac{1}{z} = \frac{c}{c^2 + d^2} - \frac{d}{c^2 + d^2} i$. The product of $\frac{1}{z}$ and $w = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i$

5. $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$. Thus $i^n = i^{\,n \bmod 4}$.

6. $\overline{z} = 3 - 4i$; $|z| = \sqrt{9 + 16} = 5$;
   $\overline{\left(\frac{1}{z}\right)} = \frac{3}{25} + \frac{4i}{25}$ and $\left|\frac{1}{z}\right| = \frac{1}{5}$;
   $\overline{z}^2 = -7 - 24i$ and $|z^2| = 25$.

7. If $z = a + bi$, then both $|z|^2$ and $\overline{z}\, z$ are equal to $a^2 + b^2$.

8. Let $z = a + bi$ and $w = x + yi$. Then

   i. Both $\overline{z} + \overline{w}$ and $\overline{(z + w)}$ are equal to $(a + x) - (b + y)i$.

   ii. Both $\overline{z}\ \overline{w}$ and $\overline{(zw)}$ are equal to $(ax - by) - (ay + xb)i$.

   iii. Both $\overline{\left(\frac{1}{w}\right)}$ and $\frac{1}{\overline{w}}$ are equal to $\frac{x + iy}{x^2 + y^2}$.

9. Since $\sqrt{3} + i = 2\left(\cos\left(\frac{p}{6}\right) + i \sin\left(\frac{p}{6}\right)\right)$, $(\sqrt{3} + i)^5 = 2^5\left(\cos\left(\frac{5p}{6}\right) + i \sin\left(\frac{5p}{6}\right)\right) =$
   $-16\sqrt{3} + 16i$. Since $(1 + i) = \sqrt{2}\cos\left(\frac{p}{4}\right) + i \sin\left(\frac{p}{4}\right)$, $(1 + i)^n =$
   $\left(\sqrt{2}\right)^n\left(\cos\left(\frac{pn}{4}\right) + i \sin\left(\frac{pn}{4}\right)\right)$, for $n = 1, 2, \ldots$

10. Applying the quadratic formula to $x^2 + x + 1$, the cube roots of 1 are 1, $\frac{-1+i\sqrt{3}}{2}$, and $\frac{-1-i\sqrt{3}}{2}$. This agrees with de Moivre's formulas since $\cos(0)+\sin(0)i = 1$, $\cos\left(\frac{2p}{3}\right)+\sin\left(\frac{2p}{3}\right)i = \frac{-1+i\sqrt{3}}{2}$ and $\cos\left(\frac{4p}{3}\right)+\sin\left(\frac{4p}{3}\right)i = \frac{-1-i\sqrt{3}}{2}$.

11. The sixth roots of unity are as follows:
$\cos(0) + \sin(0)i = 0$
$\cos\left(\frac{2p}{6}\right)+\sin\left(\frac{2p}{6}\right)i = \frac{1}{2}+\frac{i\sqrt{3}}{2}$
$\cos\left(\frac{4p}{6}\right)+\sin\left(\frac{4p}{6}\right)i = -\frac{1}{2}+\frac{i\sqrt{3}}{2}$
$\cos\left(\frac{6p}{6}\right)+\sin\left(\frac{6p}{6}\right)i = -1$

$\cos\left(\frac{8p}{6}\right)+\sin\left(\frac{8p}{6}\right)i = -\frac{1}{2}-\frac{i\sqrt{3}}{2}$
$\cos\left(\frac{10p}{6}\right)+\sin\left(\frac{10p}{6}\right)i = \frac{1}{2}-\frac{i\sqrt{3}}{2}$

12. $1+\sqrt{3}\,i = 2\left(\cos\left(\frac{p}{3}\right)+i\sin\left(\frac{p}{3}\right)\right)$ and its square roots are $\pm\sqrt{2}\left(\cos\left(\frac{p}{6}\right)+i\sin\left(\frac{p}{6}\right)\right)$ where $\sqrt{2}$ denotes the real, positive square root of 2.

13. $1 + i = \sqrt{2}\left(\cos\left(\frac{p}{4}\right)+i\sin\left(\frac{p}{4}\right)\right)$ and its cube roots are $2^{1/6}\left(\cos\left(\frac{p}{12}\right)+i\sin\left(\frac{p}{12}\right)\right)$, $2^{1/6}\left(\cos\left(\frac{9p}{12}\right)+i\sin\left(\frac{9p}{12}\right)\right)$, and $2^{1/6}\left(\cos\left(\frac{17p}{12}\right)+i\sin\left(\frac{17p}{12}\right)\right)$ where $2^{1/6}$ denotes the real sixth root of 2.

14. The roots of $x^2 + x + 1$ are cube roots of unity, which are also sixth roots of unity. So each root of $x^2 + x + 1$ is a root of $x^5 + x^4 + x^3 + x^2 + x + 1$.

15. We can check that for any $k > 0$, $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \ldots + 1)$ by multiplying. If $n = pq$ then $x^{pq} - 1 = (x^p)^q - 1 = (x^p - 1)((x^p)^{q-1} + (x^p)^{q-2} + \ldots + 1)$.

16. Note that $x^{24} - 1 = (x^{12} - 1)(x^{12} + 1)$ and that $x^{12} + 1 = (x^4 + 1)(x^8 - x^4 + 1)$. Since $\cos\left(\frac{p}{12}\right) + \sin\left(\frac{p}{12}\right)i$ is not a root of $x^{12} - 1$, it must be a root of $x^{12} + 1$. Since $\left(\cos\left(\frac{p}{12}\right) + \sin\left(\frac{p}{12}\right)i\right)^4 \neq -1$, $\cos\left(\frac{p}{12}\right) + \sin\left(\frac{p}{12}\right)i$ cannot be a root of $x^4 + 1$. Thus it must be a root of $x^8 - x^4 + 1$.

17. $z = \frac{-3i}{2} \pm \frac{\sqrt{-9-8i}}{2}$

**2.6 To the Teacher Tasks**

1. $\sqrt{3} + i = 2\left(\cos\left(\frac{p}{6}\right) + i\sin\left(\frac{p}{6}\right)\right) = e^{\ln(2) + ip/6}$
2. $e^{\frac{i2pn}{5}}$, $n = 0, 1, 2, 3, 4$.
3. i. $\frac{\ln(13)}{2} + i\arctan\left(\frac{3}{2}\right)$; ii. $1 + pi$; $\frac{pi}{2}$
4. A similarity: Arctan and the complex logarithm functions are both partial inverses of many to one functions. Thus we need to restrict our answers to values of $q$ that lie in an interval on which the tangent function and the complex exponential functions are one-to-one.
   A difference: the domain of the arctan function includes 0 whereas the domain of the complex logarithm function does not.

## Section 2.7

**In the Classroom: Why is the Product of Two Negatives Positive?**

2. In a ring $R$, there is an element $0 \in R$ such that $0 + x = x + 0 = x$ for all $x$ in $R$. Prove that this 0 is unique.

   Suppose $0_1$ and $0_2$ are two such elements. Then $0_1 = 0_1 + 0_2 = 0_2$.

3. Each element $x$ in a ring $R$ has an element $y$ (also in $R$), such that $x + y = y + x = 0$. Prove that each element $x$ has a unique such element $y$.

   Suppose $y_1$ and $y_2$ are both additive inverses of $x$ in $R$. Then $(y_1 + x) + y_2 = y_1 + (x + y_2)$, by associativity. So $(y_1 + x) + y_2 = 0 + y_2 = y_2 = y_1 + (x + y_2) = y_1 + 0 = y_1$. Thus the two inverses are equal.

## Section 2.8

1. The numbers are $5 + \sqrt{-5}$ and $5 - \sqrt{-5}$.

2. If $x = 0$ then the right hand side is 0. By making $x$ large enough we can make the left hand side greater than $q$. By continuity of polynomials, there must be an $x$ such that $x^3 + px$ exactly equals $q$.

3. If $x^3 = px + q$ has $a$ as a positive root then substitute $-a$ into the equation $x^3 + px = q$. This yields $(-a)^3 + q = p(-a)$. This becomes $-a^3 + q = -pa$. Rearrange to $a^3 = pa + q$. This is the original condition.

4. Since $\sqrt{-200} = 10\sqrt{-2}$ we can rewrite the original number as $\sqrt[3]{-4+\sqrt{-200}} + \sqrt[3]{-4-\sqrt{-200}} = \sqrt[3]{-4+10\sqrt{-2}} + \sqrt[3]{-4-10\sqrt{-2}}$. Now assume that $\sqrt[3]{-4 \pm 10\sqrt{-2}} = a \pm b\sqrt{-2}$. Keeping the positive sign and cubing both sides yields $-4+10\sqrt{-2} = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}$. By inspection $a = 2$ and $b = 1$ gives equality. Thus $\sqrt[3]{-4+10\sqrt{-2}} + \sqrt[3]{-4-10\sqrt{-2}} = (2+\sqrt{-2}) + (2-\sqrt{-2}) = 4$.

5. $\frac{1}{\sqrt{-1}} = \frac{1}{\sqrt{-1}} \cdot \frac{\sqrt{-1}}{\sqrt{-1}} = \frac{\sqrt{-1}}{-1} = -\sqrt{-1}$. With this in hand we have $\frac{\sqrt{-4}}{\sqrt{1}} = 2\sqrt{-1}$ while the other form $\frac{\sqrt{4}}{\sqrt{-1}} = \frac{2}{\sqrt{-1}} = -2\sqrt{-1}$.

## Chapter 2 Highlights: Chapter Questions

2. Reflexivity: $x$ has the same remainder as itself.
   Symmetry: If $x$ has the same remainder as $y$, then $y$ has the same remainder as $x$.

   Transitivity: If $x$ has the same remainder as $y$ and $y$ has the same remainder as $z$, then $z$ has the same remainder as $x$.

3. $[-y]_m = [m-x]_m$.

4. $42^{3335} \bmod 13 = 9$

5. i. $[4]_{15} \cup [9]_{15} \cup [14]_{15}$
   ii. $[2]_{12}$
   iii. no solution
   iv. $[156]_{211}$

6. Let $a = 15$ and $b = 19$ and $m = 10$. Then $a \bmod 10 = 5$ and $b \bmod 10 = 9$ and so $a \bmod 10 + b \bmod 10 = 14$. However, $(a + b) \bmod 10 = 34 \bmod 10 = 4$.

7. $[12]_{616}$

8. Let $d = \gcd(m, n)$. Then $m = m_1 d$ and $n = n_1 d$ for some integers $m_1$ and $n_1$. Since $a - b = qm$ and $a - b = tn$ for some integers $q$ and $t$, we have $qm = tn$ and hence $qm_1 = tn_1$. Since $\gcd(m_1, m_2) = 1$, we know that $m_1$ divides $t$ so that for some integer $s$, $t = sm_1$. Substituting in the expression $a - b = tn$, we find that $a - b = sm_1 n$. Notice that $m_1 n = mn/d = \text{lcm}(n, m)$.

9. i. 0; ii. 8; iii. 9; iv. 10

10. $13^{-1} = 4$ in $\boldsymbol{Z_{17}}$.

11. i. 16; ii. 7; iii. {2, 5, 8}

12. The units of $\boldsymbol{Z}_{15}$ are {1, 2, 4, 7, 8, 11, 13, 14}. Their inverses are, respectively,{1, 8, 4, 13, 2, 11, 7, 14}

13. In $\boldsymbol{Z_m}$, $(m-1)^{-1} = (m-1)$ because $(m-1)^2 = m^2 - 2m + 1$ and $(m^2 - 2m + 1) \bmod m = 1$.
14. An element $x$ of $\boldsymbol{Z_m}$ is zero divisor if and only if $x \neq 0$ and $\gcd(x, m) \neq 1$. In $\boldsymbol{Z}_{17}$, there are no zero divisors because 17 is prime. In $\boldsymbol{Z}_{20}$, the set of zero divisors is {2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18}.

15. An element $x$ of $\boldsymbol{Z_m}$ is a unit if and only if $\gcd(x, m) = 1$. In $\boldsymbol{Z_{17}}$, every non-zero element is a unit because 17 is prime. In $\boldsymbol{Z_{20}}$, the units are {1, 3, 7, 9, 11, 13, 17, 19}.

16. The multiplicative inverse of $1 + 3\sqrt{2}$ is $\frac{-1}{17} + \frac{3}{17}\sqrt{2}$. The solution to $(1 + 3\sqrt{2})x = 1 - 5\sqrt{2}$ is $\left(\frac{-1}{17} + \frac{3}{17}\sqrt{2}\right)\cdot\left(1 - 5\sqrt{2}\right) = \frac{-31}{17} + \frac{8}{17}\sqrt{2}$.

17. $\begin{bmatrix} 5 & -14 \\ 70 & -16 \end{bmatrix}$ Note: the answer is $x^2 + xy + yx + y^2$ and $xy \neq yx$.

18. If $p$ is not prime, then we can factor $p$ as $st$, where $s$ and $t$ are not equal to either 0 or 1 mod $p$. Thus the elements $s + 0i$ and $t + 0i$ are a zero divisors. Now suppose $p$ is prime and let $a + ib$ be an element of $\boldsymbol{Z_p}$. If $a^2 + b^2 = 0 \bmod p$ then $(a + bi)(a - bi) = 0 \bmod p$ and $(a + bi)$ cannot be a unit. On the other hand, if $a^2 + b^2 \neq 0 \bmod p$, then $a^2 + b^2$ has a multiplicative inverse $z$ in $\boldsymbol{Z_p}$. The multiplicative inverse of $(a + bi)$ is then $za - bzi$ because $(a + bi)(za - zbi) = z(a^2 + b^2) = 1$.

19. $\overline{z} = 2 + 5i$; $z + w = 3 - 7i$; $zw = -8 - 9i$; $z/w = 12/5 - i/5$; $w^2 = -3 - 4i$ ; $z^3 = -142 + 65i$.

20. $z = \frac{-1}{2} - \left(1 - \frac{\sqrt{3}}{2}\right)i$ and $z = \frac{-1}{2} - \left(1 + \frac{\sqrt{3}}{2}\right)i$.

21. $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1) = (x-1)(x+1)(x-i)(x+i)(x^2-i)(x^2+i)$
$= (x-1)(x+1)(x-i)(x+i)\left(x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}\right)\right)\left(x + \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}\right)\right)\left(x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}i}{2}\right)\right)\left(x + \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}i}{2}\right)\right)$. So the eight roots are $\pm 1, \pm i, \pm\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}\right), \pm\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}i}{2}\right)$.

22. $i = \cos(\pi/2) + i\sin(\pi/2)$. Thus the cube roots of $i$ are as follows:

$\cos(\pi/6) + i\sin(\pi/6) = \frac{\sqrt{3}}{2} + \frac{i}{2}$

$\cos(\pi/6 + 2\pi/3) + i\sin(\pi/6 + 2\pi/3) = \frac{-\sqrt{3}}{2} + \frac{i}{2}$

$\cos(p/6 + 4p/3) + i \sin(p/6 + 4p/3) = -i$.

# *Chapter 3*_____

## Section 3.1

1. $x^2 + 3x + 1$ and $x^2 + 1$
2. In $\boldsymbol{Z}_2$, there are 4 polynomials of degree 2, 4 monic. In $\boldsymbol{Z}_5$, there are 100 polynomials of degree 2, 25 monic; in $\boldsymbol{Z}_n$, there are $(n-1)n^2$ polynomials of degree 2, $n^2$ monic.

3. a. sum: $2x^2 + 6x + 3$; product: $6x^3 + 13x^2 + 9x + 2$
   b. sum: $2x^2 + x + 3$; product: $x^3 + 3x^2 + 4x + 2$
   c. sum: $2x^2 + x$; product: $x^3 + 2x^2 + 2$
   d. sum: $(2 + 3i)x^2 + 6x + 3i$ product: $(6 + 9i)x^3 + (3 + 4i)x^2 + 9ix - 2$

4. The results follow from Chapter 2.1, Theorem 2. For the $i^{\text{th}}$ coefficient of the sum, we know that $(a_i + b_i) \bmod n = (a_i \bmod n + b_i \bmod n) \bmod n$. For the $i^{\text{th}}$ coefficient of the product we know that $\left( \sum_{j+q=i} a_j b_q \right) \bmod n = \left( \sum_{j+q=i} (a_j \bmod n)(b_q \bmod n) \right) \bmod n$.

5. i. quotient: $x^2 + x + 1$; remainder: 0
   ii. quotient: $x^{n-1} + x^{n-2} + \ldots + x + 1$; remainder: 0
   iii. quotient: $2x^2 + 4x + 4$; remainder: 2
   iv. quotient: $x^3 + x^2 + 1$; remainder: 0
   v. quotient: $x^2 + x + 2 + 2i$ remainder: $3 + 2i$

6. Let $p(x) = a_n x^n + ..+ a_0$ and $q(x) = b_m x^m + \ldots + b_0$ with $a_n \neq 0$ and $b_m \neq 0$. If $a_n b_m \neq 0$, then $p(x)q(x) = a_n b_m x^{m+n} + \ldots + a_0 b_0 \neq 0$ in $R[x]$. Conversely, if $a_n b_m = 0$, then the product of the non- zero polynomials $p(x) = a_n x^n$ and $q(x) = b_m x^m$ is zero: $(a_n x^n)(b_m x^m) = (a_n b_m) x^{n+m} = 0$.

7. i. yes; ii. no; iii. no

8. Each iteration of division by $p(x) = b_m x^n + \ldots + b_0$ requires that we obtain $g_i(x) = g(x) - \frac{a_{n_i}}{b_m} x^{n-m} p(x)$ where $a_{n_i}$ is the leading coefficient of $g_{i-1}(x)$. Only the leading coefficient of $p(x)$, namely $b_m$, must be a unit for this to be carried out.

9. 0 (Use the remainder theorem and simply evaluate the polynomial at $x = 1$.)

10. 4

11. $3x^2 + 3x$. Its roots are 0, 1, 2, 3, 4, and 5.

12. All polynomials $p(x) = x^n + \ldots. + a_0$ for which $a_0 = 0$ have root 0; otherwise, all polynomials with an even number of non-zero coefficients have root 1.

13. Monic: $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$; Not monic: $2x^2 + 2$, $2x^2 + 2x + 1$, and $2x^2 + x + 1$.

14. $f(x) = q(x)(x - a) + r_0$ and $f(a) = r_0$. So $f(a) = 0$ if and only if $r_0 = 0$. Thus $f(a) = 0$ if and only if $f(x) = q(x)(x - a)$.

15. Let $n = 1$. A polynomial of the form $x - a$ has exactly one root, namely $a$. Assume that the theorem is true for polynomials of degree less than $n$ and suppose that $p(x)$ is a polynomial of degree $n > 1$. If $p(x)$ has no roots, then we are done since $0 < n$. If $p(x)$ has a root at $x_0$, then $p(x) = g(x)(x - x_0)$ and deg $(g(x)) = n - 1$. By the induction hypothesis, $g(x)$ has at most $n - 1$ roots. Any root of $p(x)$ is either equal to $x_0$ or it is a root of $g(x)$. Thus $p(x)$ has at most $n$ roots.

16. Suppose that $p - 1 = nd$ and let $y = x^d$. Then $x^{p-1} - 1 = y^n - 1 = (y - 1)(y^{n-1} + y^{n-2} + \ldots + 1)$ $= (x^d - 1)(x^{d(n-1)} + x^{d(n-2)} + \ldots + 1)$. Conversely, if $p - 1 = nd + r$ and $0 < r < d$, then the remainder of $x^{p-1} - 1$ after division by $x^d - 1$ is $x^r - 1$. (At each stage in long division, another copy $d$ is subtracted from the exponent $p - 1$ until $r$ is left.)

### 3.1 To the Teacher Tasks

1. Yes! Let $p(x) = x^2 + x + 1$. Then $p(1) = 3$, $p(2) = 7$; $p(3) = 13$ but $p(4) = 21$.
2. $(x^2 + x + 1)(x^2 + 2) + (x + 3) = x^4 + x^3 + 3x^2 + 3x + 5$ In base 10, we have $11335 = 111 \cdot 102 + 13$.

   The base 13 expression $11335 = 111 \cdot 102 + 13$ means $(13^4 + 13^3 + 3 \cdot 13^2 + 3 \cdot 13 + 5) = (13^2 + 13 + 1)(13^2 + 2) + 13 + 3$ or , in base ten, $31309 = 183 \cdot 171 + 16$.

   In base 7, the expression$11335 = 111 \cdot 102 + 13$ means $(7^4 + 7^3 + 3 \cdot 7^2 + 3 \cdot 7 + 5) = (7^2 + 7 + 1)(7^2 + 2) + 7 + 3$ or $2917 = 57 \cdot 51 + 10$.

3. Suppose that $p(x) = g(x)f(x)$ and let $m$ be an integer. For $p(m)$ to be prime, either $f(m)$ or $g(m)$ must equal 1 or – 1. But this can happen for at most a finite number of values of $m$. For instance, $f(x) = 1$, or equivalently, $f(x) - 1 = 0$ has only a finite number of solutions.

### Section 3.2

1. $(x^5 + x^4 + x^3 - 2x^2 - 2x - 2) = x(x^4 + x^3 - x^2 - 2x - 2) + (2x^3 - 2)$
   $(x^4 + x^3 - x^2 - 2x - 2) = (x/2 + 1/2)(2x^3 - 2) + (-x^2 - x - 1)$
   $(2x^3 - 2) = (-2x + 2)(-x^2 - x - 1) + 0$
   Thus $(-x^2 - x - 1) = \gcd(f, g)$ and therefore $x^2 + x + 1$ is "the" $\gcd(f, g)$.

2. $f(x) = g(x)q(x) + r(x)$ and $f(x) - g(x)q(x) = r(x)$. Thus $d(x)$ divides both $f(x)$ and $g(x)$ if and only if $d(x)$ divides both $r(x)$ and $g(x)$.
3. i. $x - 2$
   ii. $x + 4$
   iii. 1
4. $s(x)f(x) + t(x)g(x) = \gcd(f, g)$
   i. $s(x) = \frac{2}{5}x^2 - \frac{1}{10}x - \frac{1}{10}$ and $t(x) = \frac{-2}{5}x - \frac{11}{10}$