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 $(n + 1)^{\text{th}}$ 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 Σ be the set of integers greater than n_0. Let T be the subset Σ 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
*	* * * *	* * * * * * * * *	* * * * * * * * * * * * * * * *

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 · 341+202 in base five. In base 12, we let ten = T, and eleven = E. Then 42321 = 130 · 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 ith 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

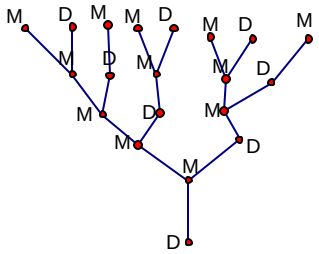
Task 1.

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