I worked alone without getting any help, except asking questions on Piazza and reading the Notes of this course.

1 Modular Arithmetic Solutions

(a) $x = 10$

Since $2, 15 \in \mathbb{Z}^+$ and $\gcd(2,\ 15) = 1$, using Theorem 6.2, we have that 2 has a multiplicative inverse, $2^{-1} \pmod{15}$, and it is unique (in the modular setting). Since we have that $2 * 8 = 16 \equiv 1 \pmod{15}$, so $2^{-1} = 8 \pmod{15}$. Then, to compute the solution to $2x \equiv 5 \pmod{15}$, we have that $x = 2^{-1} * 5 = 8 * 5 = 40 \equiv 10 \pmod{15}$, and this solution would be unique modulo 15 as well. Thus, $x = 10$ is the only solution.

(b) No solution.

We proceed by contradiction. Assume that $x \in \mathbb{Z}$ is a solution to the equation, such that $2x = y \equiv 5 \pmod{16}$, so $y \in \mathbb{Z}$.

Since $x \in \mathbb{Z}$, so we have that $2x$ is an even number. On the other hand, consider the right side of the equation, since $y \equiv 5 \pmod{16}$, so $y = 16k + 5, k \in \mathbb{Z}$. Then, since $y = 16k + 5 = 2(8k + 2) + 1$ where $8k + 2 \in \mathbb{Z}$, so we have that y is an odd number, which implies that $x \neq y$, and we reach a contradiction. Therefore, we conclude that there is no solution to this equation.

(c) $x = 2, 7, 12, 17, 22$

Let x be a solution to the equation. By definition of modular arithmetic, so we have that $0 \leq x < 25$ and $x \in \mathbb{N}$. Using the given equation, let $5x = y \equiv 10 \pmod{25}$, so $y \in \mathbb{N}$. Then, let $y = 25k + 10$, so $k \in \mathbb{N}$. Now, we have that $5x = 25k + 10$, and dividing both sides by 5, we would get $x = 5k + 2$. Since $x < 25$, so $x = 5k + 2 < 25$, so $k < \frac{23}{5}$. Since $k \in \mathbb{N}$, so k can only be $=$ 0, 1, 2, 3 and 4, with x being 2, 7, 12, 17 and 22, respectively. Thus, the only solutions are $x = 2, 7, 12, 17, 22$.

2 Euclid's Algorithm

(a) gcd(527, 323) = **17**

Step (Recursive Call)	x	y
1	527	323
2	323	204
3	204	119
4	119	85
5	85	34
6	34	17
7	17	0

And then 17 would be returned, so the greatest common divisor is 17.

(b) $5^{-1} \equiv \mathbf{11} \pmod{27}$

We would like to implement the extended Euclid's algorithm on 27 and 5.

Step (Recursive Call)	x	y	Return
1	27	5	$(1, -2, 11)$
2	5	2	$(1, 1, -2)$
3	2	1	$(1, 0, 1)$
4	1	0	$(1, 1, 0)$

And then $(1, -2, 11)$ would be returned, so we have that $\gcd(27, 5) = 1 = -2 * 27 + 11 * 5$.
Thus, $5^{-1} \equiv 11 \pmod{27}$.

(c) $x = \mathbf{17}$

Since we have that $5x + 26 \equiv 3 \pmod{27}$, so we have that $5x \equiv -23 \equiv 4 \pmod{27}$. Then, since we have from part (b) that $5^{-1} \equiv 11 \pmod{27}$, which is equivalent to $5 * 11 \equiv 1 \pmod{27}$, so we have that $5 * 11 * 4 \equiv 4 \pmod{27}$. Thus, $x = 11 * 4 = 44 \equiv 17 \pmod{27}$, so $x = 17$.

(d) Disprove

I will proceed by providing a counterexample. Consider $a = 1, b = 0, c = 1, x = 0$.

For any $x \in \mathbb{Z}$, we have that $ax = 1x = cx + 0$, which means that $ax \bmod c$ would always be 0, which implies that a has no multiplicative inverse mod c, as indicated by the hypothesis of our preposition. Then, consider $x = 0$, by definition of modular arithmetic, we have that $ax = 1 * 0 = 0 \equiv b \pmod{c}$, so $x = 0$ is a solution to the equation $ax \equiv b \pmod{c}$. Thus, $a = 1, b = 0, c = 1, x = 0$ is a counterexample.

3 Modular Exponentiation

(a) 1

Since $13 = 1 * 12 + 1$, so we have that $13 \equiv 1 \pmod{12}$, and that $1^{2018} = 1$.
So, $13^{2018} \equiv 1^{2018} \equiv 1 \pmod{12}$.

(b) 8

Since $8^2 = 64 = 7 * 9 + 1$, so we have that $8^2 \equiv 1 \pmod 9$, and that again, any power of 1 is 1.
So, $8^{11111} = 8^{2*5550+1} = (8^2)^{5550} * 8 \equiv 1 * 8 \equiv 8 \pmod 9$.

(c) 4

Since we have that:
$7^2 = 49 \equiv 5 \pmod{11}$,
$7^4 \equiv 5^2 = 25 \equiv 3 \pmod{11}$,
$7^8 \equiv 3^2 = 9 \equiv 9 \pmod{11}$,
$7^{16} \equiv 9^2 = 81 \equiv 4 \pmod{11}$,
$7^{32} \equiv 4^2 = 16 \equiv 5 \pmod{11}$,
$7^{64} \equiv 5^2 = 25 \equiv 3 \pmod{11}$,
$7^{128} \equiv 3^2 = 9 \equiv 9 \pmod{11}$,
Thus, $7^{256} \equiv 9^2 = 81 \equiv 4 \pmod{11}$.

(d) 16

Since we have that:
$3^2 = 9 \equiv 9 \pmod{23}$,
$3^4 = 9^2 = 81 \equiv 12 \pmod{23}$,
$3^8 = 12^2 = 144 \equiv 6 \pmod{23}$,
$3^{16} = 6^2 = 36 \equiv 13 \pmod{23}$,
$3^{32} = 13^2 = 169 \equiv 8 \pmod{23}$,
$3^{64} = 8^2 = 64 \equiv 18 \pmod{23}$,
$3^{128} = 18^2 = 324 = 14 * 23 + 2 \equiv 2 \pmod{23}$.
Thus, $3^{160} = 3^{128+32} = 3^{128} * 3^{32} \equiv 2 * 8 \equiv 16 \pmod{23}$.

4 Euler's Totient Function

(a) $p - 1$

Since p is a prime number, by definition of prime numbers, so $p > 1$ and p is not divisible by any positive integer except 1 and itself, p. First, by definition of greatest common divisor, we have that $\gcd(p, 1) = 1$ and $\gcd(p, p) = p \neq 1$, which means that 1 is in the set we defined, and p is not. We proceed to prove that for any arbitrary $i \in \mathbb{N}, 1 < i < p$, we have that $\gcd(p, i) = 1$, which is equivalent to i is in the set.

Assume, for a contradiction, that $\gcd(p, i) \neq 1$. Let $\gcd(p, i) = d$, so $d > 1, d \in \mathbb{N}$ and $d \mid p$. Also, since $i < p$, so $d \neq p$, so $1 < d < p$ and $d \mid p$. But, by definition of primes, p should not be divisible by any positive integer besides 1 and p, and we reach a contradiction.

Thus, for all $i \in \mathbb{N}, 1 < i < p$, we have that $\gcd(p, i) = 1$, which means that i is in the set by definition of Euler's totient function.

Therefore, there is a total of $1 + (p - 2) = p - 1$ positive integers less than or equal to p which are relatively prime to it; in other words, $\phi(p) = p - 1$.

(b) $p^k - p^{k-1}$

Since p is a prime, so the only prime factor of p^k is p. We claim that for any integer $i\mathbb{Z}^+, 1 \leq i \leq p^k$, if i is relatively prime to p, then i is also relatively prime to p^k. We proceed by contradiction to prove the claim.

Suppose there exist an $i^*\mathbb{Z}^+, 1 \leq i^* \leq p^k$ such that i^* is relatively prime to p, but not relatively prime to p^k. Let $\gcd(p^k, i^*) = d$, so $d \in \mathbb{Z}, d > 1$. So, we have that $d \mid i^*$ and $d \mid p^k$, and since p is a prime, so d would have to divide p. Now, $d \mid p$ and $d \mid i^*$, so $\gcd(p, i^*) > d > 1$, which implies that p, i^* are not relatively prime, so we conclude with a contradiction, so our assertion above is true.

Thus, if i is in the set we defined, meaning that p^k, i are relatively prime, then p, i are also relatively prime. Using the logic from our proof in part (a), since p is a prime, so i would be relatively prime to p^k unless $p \mid i$; in other words, i is a multiple of p. For i such that $1 \leq i \leq p^k$, since $p^k = p^{k-1} * p$, so all the multiples of p are: $1 * p, 2 * p, 3 * p, ..., p^{k-1} * p$, which means that there are p^{k-1}-many multiples of p, and all other positive integers less than or equal to p^k are relatively prime to p^k. Thus, there are $p^k - p^{k-1}$ numbers relatively prime to p^k.

Therefore, there are $(p^k - p^{k-1})$-many numbers in the set defined; so in other words, $\phi(p^k) = p^k - p^{k-1}$.

(c) 1

Since p is a prime number and $a \in \mathbb{Z}^+, a < p$, using our logic in parts (a) and (b) again, so we have that a, p are relatively prime. Again, using the result from part (a), so we have that $\phi(p) = p - 1$. With the fact that we proved earlier, which is equivalent to $\gcd(p, a) = 1$, using *Fermat's Little Theorem*, so we have that $a^{\phi(p)} \equiv 1 \pmod{p}$.

(d) Direct Proof

We proceed by a direct proof. Given that $b \in \mathbb{Z}^+$ with prime factors $p_1, p_2, ..., p_k$, and $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, so we have that $p_1, p_2, ..., p_k$ are all different primes, which implies that $p_1, p_2, ..., p_k$ are all relatively prime; in other words, for any p_i, p_j with $1 \leq i, j \leq k$, so $\gcd(p_i, p_j) = 1$. Now we claim that for two different primes p_i, p_j, then for any $\alpha_i, \alpha_j \in \mathbb{N}$, we have $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$.

Assume, for a contradiction, that $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) \neq 1$, so let $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = d$ where $d \in \mathbb{Z}^+, d > 1$.

Thus, we have that $d \mid p_i^{\alpha_i}$. Since p_i is prime and $d > 1$, so d has to be a multiple of p_i. Let $d = p_i \cdot d^*, d^* \in \mathbb{Z}^+$. Since by definition of greatest common divisors, we also have that $d \mid p_j^{\alpha_j}$, so $p_i \mid p_j^{\alpha_j}$, which is impossible since p_i, p_j are different primes. Thus, we have a contradiction, so $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$.

Thus, using the given property of Euler's totient function, we have that $\phi(b) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$. Then, using the result obtained from part (b), we have that $\phi(b) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$.

Now, for any a relatively prime to b, and any arbitrary $i \in \{1, 2, ..., k\}$, we have that a, p_i is also relatively prime, which is equivalent to $\gcd(a, p_i) = 1$. Thus, *Fermat's Little Theorem*, we have that $a^{p_i - 1} \equiv 1 \pmod{p_i}$.

Therefore, $a^{\phi(b)} = a^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} = a^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_i^{(\alpha_i - 1)} \cdot (p_i - 1)) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} = a^{(p_i - 1) \cdot (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots p_i^{(\alpha_i - 1)} \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} \equiv 1^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots p_i^{(\alpha_i - 1)} \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} \equiv 1 \pmod{p_i}$.

Therefore, for any a relatively prime to b, $\forall i \in \{1, 2, ..., k\}, a^{\phi(b)} \equiv 1 \pmod{p_i}$.

Q.E.D.

5 FLT Converse

(a) Direct proof

Proof. We proceed by a direct proof. For any a that's not relatively prime to n, let $\gcd(a, n) = d, d > 1$. Let $a = d \cdot a^*, n = d \cdot n^*$. For any $x \in \mathbb{Z}$, let $ax = kn + y, k \in \mathbb{Z}, 0 \le y < n$. By definition of modular arithmetic, we have that $ax \equiv y \pmod{n}$. Substituting, we have that $d \cdot a^* \cdot x = k \cdot d \cdot n^* + y$. Since $d \mid (d \cdot a^* \cdot x)$, so $d \mid (k \cdot d \cdot n^* + y)$, so we can infer that $d \mid y$. Since $d > 1$, so $y > 1$, and since $0 \le y < n$, so we have proved that any multiple of a mod n would not be 1. Thus, $a^{n-1} = a \cdot a^{n-2} \not\equiv 1 \pmod{n}$.

Q.E.D.

(b) Direct proof

Proof. We proceed by a direct proof. Suppose we have some $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$. Consider any $x \in S(n)$ such that $x^{n-1} \equiv 1 \pmod{n}$, we claim that for $k \equiv ax \pmod{n}$ where $1 \le k \le n$, we have that k is another such a, i.e. $k \in S(n)$ and $k^{n-1} \not\equiv 1 \pmod{n}$.

First, we'll show that $k \in S(n)$. On the one hand, we have defined that $1 \le k \le n$. On the other hand, since $a, x \in S(n)$, so we have that $\gcd(n, a) = 1$ and $\gcd(n, x) = 1$, which would give us that $\gcd(n, ax) = 1$, so $\gcd(n, k) = 1$. Thus, by definition of the set $S(n)$, so $k \in S(n)$.

Then, since $a^{n-1} \not\equiv 1 \pmod{n}$, $x^{n-1} \equiv 1 \pmod{n}$ and $k \equiv ax \pmod{n}$, so we have that $k^{n-1} \equiv (ax)^{n-1} = a^{n-1} \cdot x^{n-1} \equiv a^{n-1} \cdot 1 = a^{n-1} \not\equiv 1 \pmod{n}$.

Thus, we have proved if we can find some $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, then for any $x \in S(n)$ such that $x^{n-1} \equiv 1 \pmod{n}$, we have a corresponding $k \in S(n)$ such that $k^{n-1} \not\equiv 1 \pmod{n}$. Also note that since $\gcd(a, n) = 1$, so for any two different $x \in S(n)$ (namely, $1 \le x \le n$), then ax is unique mod n, which implies that the k we constructed would be unique for different n. In other words, we have an injection from the set of numbers in $S(n)$ that pass the FLT condition to the set of numbers in $S(n)$ that fail it. This implies that the set of numbers in $S(n)$ that fail the FLT condition is at least as large as the set of numbers in $S(n)$ that pass it.

Therefore, we have that if we can find a single $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, then we can find at least $|S(n)|/2$ such a.

Q.E.D.

(c) Direct proof

Proof. We proceed by a direct proof. Let $a, b, m_1, m_2 \in \mathbb{Z}$ such that $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}$ and $\gcd(m_1, m_2) = 1$. So, we have that $(a - b) \equiv 0 \pmod{m_1}$ and $(a - b) \equiv 0 \pmod{m_2}$, which is equivalent to $m_1 \mid (a - b)$ and $m_2 \mid (a - b)$.

So, let $(a - b) = m_1 k$ where $k \in \mathbb{Z}$, and we have that $m_2 \mid (m_1 k)$. And since we are given that $\gcd(m_1, m_2) = 1$, so we have $m_2 \mid k$. Let $k = m_2 k^*, k^* \in \mathbb{Z}$. So, $(a - b) = m_1 k = m_1 m_2 k^*$ is a multiple of $m_1 m_2$. In other words, $(m_1 m_2 \mid (a - b)$, which implies that $a \equiv b \pmod{m_1 m_2}$, as desired.

Q.E.D.

(d) Direct proof

Proof. We proceed by a direct proof. Let $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $(p_i - 1) \mid (n - 1)$ for all $i, 1 \le i \le k$. Let a be an arbitrary element such that $a \in S(n)$. Thus, by our definition of $S(n)$, we have that $\gcd(n, a) = 1$. We claim that a is not the multiple of any p_x where $1 \le x \le k$.

Suppose, for a contradiciton, that for some $1 \le x \le k$, we have $p_x \mid a$. Since we also have that $p_x \mid n$, so p_x is a common divisor for a, n, which means that $\gcd(n, a) > p_i > 1$, which causes a contradiction.

Thus, we have proved that a is not the multiple of any p_x where $1 \leq x \leq k$. Thus, for any $1 \leq j \leq k$, so a is coprime with any p_j. Let $a \equiv a_j \pmod{p_j}$, so $1 \leq a_j \leq (p_j - 1)$. Using Fermat's Little Theorem, so we have that $a^{p_j - 1} \equiv a_j^{p_j - 1} \equiv 1 \pmod{p_j}$.

Since $1 \leq j \leq k$, so we know that $(p_j - 1) \mid (n - 1)$. Let $n - 1 = d_j(p_j - 1)$, $d_j \in \mathbb{Z}$. Thus, $a^{n-1} = a^{d_j(p_j - 1)} = (a^{p_j - 1})^{d_j} \equiv 1^{d_j} \equiv 1 \pmod{p_j}$. Since p_j is picked arbitrarily, so we could reduce that for all $1 \leq j \leq k$, we have that $a^{n-1} \equiv 1 \pmod{p_j}$. Then, since we have that p_i are distinct primes, for any two p_p, p_q where $1 \leq p, q \leq k$, so $\gcd(p_p, p_q) = 1$. Then, since we just proved that $a^{n-1} \equiv 1 \pmod{p_p}$ and $a^{n-1} \equiv 1 \pmod{p_q}$, using the result of part (c) above, so we have that $a^{n-1} \equiv 1 \pmod{p_p p_q}$. Thus, repeat this process for all p_i where $1 \leq i \leq k$, so we have that $a^{n-1} \equiv 1 \pmod{p_1 p_2 \cdots p_k}$. Since $n = p_1 p_2 \cdots p_k$, so this is equivalent to $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$.

Q.E.D.

(e) Direct proof

Proof. We proceed by a direct proof. Using prime factorization, so $561 = 3 \cdot 11 \cdot 17$. Since we also have that $3 - 1 = 2, 11 - 1 = 10, 17 - 1 = 16, 561 - 1 = 560$, and that $560 = 280 \cdot 2 = 56 \cdot 10 = 35 \cdot 16$, so we have that $(3 - 1) \mid (561 - 1), (11 - 1) \mid (561 - 1)$, and $(17 - 1) \mid (561 - 1)$.

Thus, for all $x \in S(561)$, which is equivalent to x being coprime with 561 and $1 \leq x \leq 561$, using our result from part (d), we have that $x^{560} \equiv 1 \pmod{561}$.

Thus, for all a that is coprime with 561, let $a \equiv a_{mod} \pmod{561}$ where $1 \leq a_{mod} \leq 561$. Then, using our proof for the Euclidean algorithm, we have that $\gcd(561, a_{mod}) = \gcd(561, a) = 1$. Thus, by definition, we have that $a_{mod} \in S(561)$. So, $a^{560} \equiv a_{mod}^{560} \equiv 1 \pmod{561}$.

Therefore, we have shown that for all a coprime with 561, $a \equiv 1 \pmod{561}$.

Q.E.D.