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 $ax = kn + y, k \in \mathbb{Z}, 0 \leq y < n$. 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 $0 \leq y < n$, 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 $1 \leq k \leq n$, 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 $1 \leq k \leq n$. 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, $1 \leq x \leq n$), 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 $i, 1 \leq i \leq k$. 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 $1 \leq x \leq k$.

Suppose, for a contradiciton, that for some $1 \leq x \leq k$, 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.