Theorem: The pairing output by the Stable Marriage algorithm is male optimal.

Proof: Suppose for the sake of contradiction that the pairing is *not* male optimal. Assume the first day when a man got rejected by his optimal woman was day k. On this day, M was rejected by W^* (his optimal mate) in favor of M^* who proposed to her. By definition of optimal woman, there must be exist a stable pairing T in which M and W^* are paired together. Suppose T looks like this: $\{\ldots,(M,W^*),\ldots,(M^*,W'),\ldots\}$. We will argue that (M^*,W^*) is a rogue couple in T, thus contradicting stability.

First, it is clear that W^* prefers M^* to M, since she rejected M in favor of M^* during the execution of the stable marriage algorithm. Moreover, since day k was the first day when some man got rejected by his optimal woman, on day k M^* had not yet been rejected by his optimal woman. Since he proposed to W^* on the k-th day, this implies that M^* likes W^* at least as much as his optimal woman, and therefore at least as much as W'. Therefore, (M^*,W^*) form a rogue couple in T, and so T is not stable. Contradiction. Thus, our assumption was wrong and the pairing is male optimal. ♠

Let us return to proving that $D(E(x)) = x$:

Theorem 4.2: Under the above definitions of the encryption and decryption functions E and D, we have $D(E(x)) = x \bmod N$ for every possible message $x \in \{0,1,\ldots,N-1\}$.

The proof of this theorem relies on Fermat's Little Theorem:

Proof of Theorem 6.2: To prove the statement, we have to show that

$$(x^e)^d = x \bmod N \qquad \text{for every } x \in \{0,1,\ldots,N-1\}. \tag{1}$$

Let's consider the exponent, which is ed. By definition of d, we know that $ed = 1 \bmod (p-1)(q-1)$; hence we can write $ed = 1 + k(p-1)(q-1)$ for some integer k, and therefore

$$x^{ed} - x = x^{1+k(p-1)(q-1)} - x = x(x^{k(p-1)(q-1)} - 1). \tag{2}$$

Looking back at equation (1), our goal is to show that this last expression in equation (2) is equal to 0 mod N for every x.

Now we claim that the expression $x(x^{k(p-1)(q-1)} - 1)$ in (2) is divisible by p. To see this, we consider two cases:

Case 1: *x is not a multiple of p.* In this case, since $x \neq 0 \bmod p$, we can use Fermat's Little Theorem to deduce that $x^{p-1} = 1 \bmod p$. Then $(x^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \bmod p$ and hence $x^{k(p-1)(q-1)} - 1 = 0 \bmod p$, as required.

Case 2: *x is a multiple of p.* In this case the expression in (2), which has x as a factor, is clearly divisible by p.

By an entirely symmetrical argument, $x(x^{k(p-1)(q-1)} - 1)$ is also divisible by q. Therefore, it is divisible by both p and q, and since p and q are primes it must be divisible by their product, $pq = N$. But this implies that the expression is equal to 0 mod N, which is exactly what we wanted to prove. □

roof of Property 1

ow let us turn to property 1: a non-zero polynomial of degree d has at most d roots.The idea of the proof s as follows. We will prove the following claims:

Claim 1 If a is a root of a polynomial $p(x)$ with degree d, then $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ with degree $d-1$.

Claim 2 A polynomial $p(x)$ of degree d with distinct roots $a_1,\ldots,a_d$ can be written as $p(x) = c(x-a_1)\cdots(x-a_d)$.

laim 2 implies property 1. We must show that $a \neq a_i$ for $i = 1,\ldots d$ cannot be a root of $p(x)$. But this ollows from claim 2, since $p(a) = c(a-a_1)\cdots(a-a_d) \neq 0$.

Lemma: The algorithm terminates with a pairing.

Proof: Suppose for contradiction that there is a man M who is left unpaired at the end of the algorithm. He must have proposed to every single woman on his list. By the Improvement Lemma, each of these women thereafter has someone on a string. Thus when the algorithm terminates, n women have n men on a string not including M. So there must be at least $n+1$ men. Contradiction. ♠

Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

Proof: Our first claim is that $f(x)$ is a bijection. We will then show that this claim implies the theorem.

To show that f is a bijection, we simply need to argue that the numbers $a \cdot i \bmod p$ are distinct. This is because if $a \cdot i \equiv a \cdot j \pmod p$, then dividing both sides by a gives $i \equiv j \pmod p$. They are nonzero because $a \cdot i \equiv 0$ similarly implies $i \equiv 0$. (And we *can* divide by a, because by assumption it is nonzero and therefore relatively prime to p.)

Now we can prove the theorem. Since f is a bijection, we know that the image of f is S. Now if we take the product of all elements in S, it is equal to the product of all elements in the image of f:

$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod p.$$

Dividing by $(p-1)!$ (which we can do because it is relatively prime to p, since p is assumed prime) then gives the theorem.

□

Improvement Lemma: If M proposes to W on the kth day, then on every subsequent day she has someone on a string whom she likes at least as much as M.

Proof: Suppose towards a contradiction that the jth day for $j > k$ is the first counterexample where W has either nobody or some M* inferior to M on a string. On day $j-1$, she has M′ on a string and likes M′ at least much as M. According to the algorithm, M′ still proposes to W on the jth day since she said "maybe" the previous day. So W has the choice of at least one man on the jth day; moreover, her best choice is at least as good as M′, and according to the algorithm she will choose him over M*. This contradicts our initial assumption. ♠

Theorem: If a pairing is male optimal, then it is also female pessimal.

Proof: Let T = {. . . , (M, W), . . . } be the male optimal pairing (which we know is output by the algorithm). Suppose for the sake of contradiction that there exists a stable pairing S = {. . . , (M*, W), . . . , (M, W′), . . . } such that M* is lower on W's list than M (i.e., M is not her pessimal man). We will argue that S cannot possibly be stable by showing that (M,W) is a rogue couple in S. By assumption, W prefers M to M* since M* is lower on her list. And M prefers W to his partner W′ in S because W is his partner in the male optimal pairing T. Contradiction. Therefore, the male optimal pairing is female pessimal. ♠

Proof of Property 2

We would like to prove property 2:

Property 2: Given $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

We have shown how to find a polynomial $p(x)$ such that $p(x_i) = y_i$ for $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$. This proves part of property 2 (the existence of the polynomial). How do we prove the second part, that the polynomial is unique? Suppose for contradiction that there is another polynomial $q(x)$ such that $p(x_i) = y_i$ for all $d+1$ pairs above. Now consider the polynomial $r(x) = p(x) - q(x)$. Since we are assuming that $q(x)$ and $p(x)$ are different polynomials, $r(x)$ must be a non-zero polynomial of degree at most d. Therefore, property 1 implies it can have at most d roots. But on the other hand $r(x_i) = p(x_i) - q(x_i) = 0$ on $d+1$ distinct points. Contradiction. Therefore, $p(x)$ is the unique polynomial that satisfies the $d+1$ conditions.

Theorem: The pairing produced by the algorithm is always stable.

Proof: We will show that no man M can be involved in a rogue couple. Consider any couple (M,W) in the pairing and suppose that M prefers some woman W* to W. We will argue that W* prefers her partner to M, so that (M,W*) cannot be a rogue couple. Since W* occurs before W in M's list, he must have proposed to her before he proposed to W. Therefore, according to the algorithm, W* must have rejected him for somebody she prefers. By the Improvement Lemma, W* likes her final partner at least as much, and therefore prefers him to M. Thus no man M can be involved in a rogue couple, and the pairing is stable. ♠