Well Ordering Principle
1. Find smallest n such that it is false for some claim.
2. Show $n-1 \to n$ is true. Thus causing a contradiction.
3. Alternatively, show that $n \to n-1$, which shows that $n-1$ was the smallest example, thus violating our initial assumption of n being the smallest.

Claim: If I draw n straight lines on a piece of paper I cannot divide the piece of paper into more than $\frac{n(n+1)}{2}+1$ regions.
Proof: We will use the well-ordering principle to find a contradiction. Consider a minimal set of lines L violating the conjecture. Since 0 lines divide the paper into $0(0+1)2+1=1$ regions, L must be non-empty. Fix some line $l \in L$. Removing l would cause some pairs of regions. Two regions are merged if and only if one of the borders they share is a segment of l. So removing l reduces the total number of regions only by the total number of segments of l. The number of segments of l is at most one more than the number of intersections of l with other lines in L. Since l can intersect each of the other $n-1$ lines at most once, l has at most n segments. Thus removing l merges at most n pairs of regions, leaving more than $\frac{n(n+1)}{2}+1-n=\frac{n(n-1)}{2}+1$ regions. But then we are left with a set of $n-1$ lines which divide the sheet of paper into more than $\frac{(n-1)n}{2}+1$ regions, contradicting our assumption that L was a minimal counterexample.

HW1, Problem 1
Claim: Suppose that $x \in R$ such that $x+\frac{1}{x} \in Q$.
Using strong induction, show that for each $n \in N$, $a_n = x_n + \frac{1}{x_n} \in Q$.
Solution: We proceed by strong induction, using $a_0 \in Q$ and $a_1 \in Q$ as our base case. (We are proving the stronger statement that $n \geq 0$ implies $a_n \in Q$.)
Base Case: $a_0 = 1+1 = 2$ is clearly in Q, and $a_1 = x + \frac{1}{x} \in Q$ by hypothesis.
Induction Hypothesis: Suppose $n \geq 1$ and that for each $0 \leq k \leq n$, $a_k \in Q$.
Induction Step: Note that $a_1 a_n = (x+\frac{1}{x})(x_n + \frac{1}{x_n})$
$= x^{n+1} + x^{n-1} + \frac{1}{n-1} + \frac{1}{n+1} = a_{n+1} + a_{n-1}$. Thus
$a_{n+1} = a_1 a_n - a_n - 1$. By the inductive hypothesis, a_1, $a_n - 1$, a_n are all rational. Thus $a_n + 1$ is a sum of products of rational numbers, and hence rational.

Polynomials, Lecture Note 5
A polynomial in a single variable is of the form
$p(x) = a_d x^d + a_{d1} x^{d1} + \cdots + a_0$.
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 $p(x_i) = y_i for 1 \leq i \leq d+1$.

Bijections, Lecture Note 4
A bijection is a function for which every $b \in B$ has a unique pre-image $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:
1. f is *onto*: every $b \in B$ has a pre-image $a \in A$.
2. f is *one-to-one*: for all a,$a' \in A$, if $f(a) = f(a')$ then $a = a'$.

RSA, Lecture Notes 4
Encryption function $E(x) \equiv x^e \bmod N$ where $N = pq$, (p and q are two large primes), $E : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ and e is relatively prime to $(p-1)(q-1)$. The inverse of the RSA function is the dycryption function: $D(x) = x^d \bmod N$ where d is the inverse of $e \bmod (p-1)(q-1)$.
Public key: (N, e)
Private key: d
$D(E(x)) = x$ (therefore $E(x)$ is a bijection)

HW2, Problem 3
Consider another scenario in which we do allow for ties. i.e. There may be several partners that are equally preferred by a person. As an example consider the scenario in which the women are indifferent amongst the men:

Men	Women
1	A > B
2	B > A

Women	Men
A	1 = 2
B	1 = 2

In this kind of scenario the definition of a stable pairing is no longer obvious. Consider the following definitions for stability criteria: As in the original problem, define a *rogue couple* to be a man and a woman who prefer each other than their partners in the pairing. We say a pairing is *stable* if it has no *rogue couple*. In the presence of ties, is there an algorithm that always yields a stable pairing? If so, prove it. If not, provide a counter example.
Solution:
One good algorithm is to use the following convention: Everyone generates a temporary ranking by breaking any ties using alphabetical/numerical order. (For instance if my ranking was $D > B = C > A$ my temporary ranking would become $D \geq B \geq C \geq A$). Use the traditional stable marriage algorithm on the temporary rankings.
Claim: This will yield a stable pairing for the original set of rankings.
Proof (By Contradiction):
The key to the proof is that if you preferred person x to person y in the temporary rankings, you will not prefer person y to person x according to your original rankings. Assume that you can actually find a *rogue couple* according to the original preferences after pairing everyone using the temporary rankings. If that is true then consider the man in the the *rogue couple*, and call him M. Call his current wife W and his preferred wife W^*. Because M and W^* form a rogue couple, he must prefer her over W and therefore his ranking of W^* must be greater than his ranking of W in the temporary system. So he must have proposed to W^* when we applied the stable marriage algorithm under the temporary rankings. Since W^* is not with M she must have rejected him for her current partner M^*. So under her temporary ranking $M^* \geq M$ which means that either she ranks M and M^* equally, or she prefers M^* to M! This is of course a contradiction because we assumed that M and W^* prefer each other to their current partners.

Modulo with Polynomials

We can use mod with polynomials. For example:
$P(x) = x^3 + 2x + 3$, and $Q(x) = x^2 + 4x + 3$. Find $P(x) * Q(x) \bmod 5$
Solution:
$P(x)Q(x) = x^5 + 4x^4 + 5x^3 + 11x^2 + 18x + 9 \bmod 5$
$= (x)(x^4) + (4)(x^4) + (0)(x^3) + (1)(x^2) + (3)x + 4 \bmod 5$
$= (x)(1) + 4(1) + x^2 + 3x + 4 \bmod 5$, since $x^{5-1} \equiv 1 \bmod 5$
$= x^2 + 4x + 8 \bmod 5$
$= x^2 + 4x + 3 \bmod 5$

Simplify: $5^{782^{258}} \bmod 22$
We can reduce the exponent first. Since $22 = 11 * 2$, we know $x^{(11-1)(2-1)} \equiv x^{10} \equiv 1 \bmod 22$, so we have:
$782^{258} \bmod 10$. Likewise, $10 = 5 * 2$, so $258 \bmod 4 \equiv 2$ in this case. Thus, $782^{258} \equiv 782^2 \bmod 10$, so we simplify to get $2^2 \bmod 10 \equiv 4$. Thus, we have
$5^{782^{258}} \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \bmod 22$

Modular Arithmetic & Properties
Theorem 3.1: If $a = c \bmod m$ and $b = d \bmod m$, then $a+b = c+d \bmod m$ and $ab = cd \bmod m$.
Proof (for addition portion of Thm. 3.1): We know that $c = a + km$ and $d = b + lm$, so $c + d = a + km + b + lm = a + b + (k+l)m$, which means that $a + b = c + d \bmod m$.
Theorem 3.2: Let m, x be positive integers such that $gcd(m, x) = 1$. Then x has a multiplicative inverse modulo m, and it is unique (modulo m).
Euclid's Algorithm
Theorem 3.3: Let $x \leq y$ and let q, r be natural numbers such $x = yq + r$ and $r < y$. Then $gcd(x, y) = gcd(r, y)$.

Stable Marriage Algorithm, Lecture Notes 2
(1) Each man goes to the first woman on his list not yet crossed off and proposes to her. (2) She says maybe to her favorite and NEVER to everyone else. (3) All the men who got "NEVER" cross off that woman and move down their list. (4) Keep going till everyone is matched. Note: A "rogue couple" is when two people in different relationships prefer each other to their current partners.

Analyis
To establish that it outputs a stable pairing, we need the following crucial lemma:
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.

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.

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 M. 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 Ms list, he must have proposed to her before he proposed to M. 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.

Theorem: The pairing output by the Stable Marriage algorithm is male optimal.
Theorem: If a pairing is male optimal, then it is also female pessimal.

Fermat's Little Theorem: For any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} = 1 \bmod p$.
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 $x \in \{0, 1, \ldots, N-1\}$.
Proof: To prove the statement, we have to show that
$(x^e)^d = x \bmod N$ for every $x \in \{0, 1, \ldots, N-1\}$. (1)
$ed = 1 \bmod (p-1)(q-1)$; hence we can write $ed = 1 + k(p-1)(q-1)$ for some integer k, and therefore
$x^{ed} - x = x^{1+k(p-1)(q-1)} - x = x(x^{k(p-1)(q-1)} - 1)$. (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 Fermats Little Theorem to deduce that $x^{p-1} = 1 \bmod p$. Then $x^{(p-1)k(q-1)} = 1^{k(q-1)} \bmod p$ 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.