Inspired by Tsion, written by Vania.

Induction and Strong Induction

Induction - show that given some clain for n, it also leads to n+1. For strong induction, assume all numbers $0 < k < n$ are true, and prove n using this assumption. Useful if the n formula can be decomposed into smaller terms, since they are already true.

Example:
Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
(1) Base case: Check for $n = 0, 1$ and (2) Assume true for n, show this leads to $n + 1$
We know: $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n + 1)$
Which means $\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + (n + 1) \rightarrow \frac{n(n+1)}{2} + \frac{2n+2}{2}$
$= \frac{n^2+3n+2}{2} \rightarrow \frac{(n+1)(n+2)}{2}$, so $n \rightarrow n + 1$

Stable Marriage

(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.

Note:
1. Male Optimal and Female pessimive, because men get choice. if (1:A,B),(2:B,A), but (A:2,1),(B:1,2), each man gets top choice but woman gets worst.
2. Women improve each day (or stay the same), while men get worse partner (or stay the same).
3. If women have ties wierd stuff happens - both men want same women and she likes both, so rogue couple for loser.
4. At most $n(n-1)+1$ proposals - each man of n men can suffer at most $(n-1)$ rejections, so $n(n-1)$, $+1$ for the last day.

Euclid and GCD

Let $x \leq y$ and let q, r be natural numbers such $x = yq + r$ and $r < y$. Then $gcd(x, y) = gcd(r, y)$.
This is because any common divisor of x and y is also a common divisor of x and r and vice versa. To see this, if d divides divides both x and y, there exist integers z and z' such that $zd = x$ and $z'd = y$. Therefore $r = x - yq = zd - z'dq = (z - z'q)d$, and so d divides r. The other direction follows in exactly the same way.

Example:
Find the GCD(23,9)
$23 = 2 * 9 + 5 \rightarrow 9 = 1 * 5 + 4 \rightarrow 5 = 1 * 4 + 1 \rightarrow 4 = 4 * 1 + 0$
Now we chain back up: $1 = 5 * 1 - 1 * 4$, and since $4 = 1 * 9 - 1 * 5$ we get $1 = 5 * 1 - 1 * (1 * 9 - 1 * 5)$. etc:
$1 = 2 * 5 - 1 * 9 \rightarrow 1 = 2 * (1 * 23 - 2 * 9) - 1 * 9 \rightarrow 1 = 2 * 23 - 5 * 9$.
Note: In this manner we have also found that $23^{-1} \equiv 2 \bmod 9$.

Modulo Properties

If $a = c \bmod m$ and $b = d \bmod m$, then $a + b = c + d \bmod m$ and $ab = cd \bmod m$.
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 $a + b = c + d \bmod m$.
Let m, $x > 0 \in \mathbb{Z}$ and $gcd(m, x) = 1$. Then $\exists x^{-1} \bmod m$, and it is unique $\bmod m$.

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 $5^{782^{258}} \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \bmod 22$

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 $x^{5-1} \equiv 1 \bmod 5$
$= x^2 + 4x + 8 \bmod 5$
$= x^2 + 4x + 3 \bmod 5$

Secret Sharing

A polynomial in a single variable is of the form $p(x) = a_d x^d + a_{d1} x^{d1} + \cdots + a_0$.
A non-zero polynomial of degree d has at most d roots.
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 $p(x_i) = y_i for 1 \leq i \leq d + 1$.
Explanation: Polynomial is evaluated at $P(x) for 1 < x < k$, values are given out to k individuals. They can then get at least $d + 1$ people and extrapolate the original polynomial.

Example:
Given these three points find the polynomial: (1,0) (2, 1), (3,1)
$\Delta x_1 = ((x - 2)(x - 3))/((1 - 2)(1 - 3))$
$\Delta x_2 = ((x - 1)(x - 3))/((2 - 1)(2 - 3))$
$\Delta x_3 = ((x - 1)(x - 2))/((3 - 1)(3 - 2))$
$P(x) = y_1 \Delta x_1 + y_2 \Delta x_2 + y_3 \Delta x_3$

Well Ordering Principle

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

RSA and Bijections

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

Fermat's Little Theorem: For any prime p and any $a \in \{1, 2, \ldots, p - 1\}$, we have $a^{p-1} = 1 \bmod p$.
Additionally, $x^{(P-1)(Q-1)} \bmod N \equiv 1$, with $N = PQ$, and P,Q are prime.

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

The security of RSA hinges upon the following simple assumption:
Given N, e and $y = x^e \bmod N$, there is no efficient algorithm for determining x.

Polynomials

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 $p(x_i) = y_i for 1 \leq i \leq d + 1$.

1. Relax
2. You will do GREAT!
3. The "A" is yours!