1. Fibonacci numbers. The Fibonacci numbers F_n are defined by

$$F_1 = 1, \qquad F_2 = 1, \qquad F_{n+2} = F_{n+1} + F_n \quad (n \geq 1).$$

---

2. RSA.

(a) Numerization key.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

(b) Encoding. To compute $n^k \pmod{m}$:

- **Step 1.** Compute the binary expansion of k (write k as a sum of powers of 2, including, if necessary, the power $2^0 = 1$).
- **Step 2.** Make a list of the base n raised to successive powers of 2 (starting with $2^0 = 1$), $\pmod{m}$. Keep going until you've raised n to the largest power of 2 appearing in Step 1. Each entry in the list is found by squaring, and reducing $\pmod{m}$, the previous entry.
- **Step 3.** Put Steps 1 and 2 together to compute $n^k \pmod{m}$, reducing along the way to keep numbers small.

(c) Decoding. To decode the message b:

- **Step 1.** Find natural numbers x and y such that

$$kx - \varphi(m)y = 1.$$

  (See item 3, "The Euclidean Algorithm," below.)
- **Step 2.** Compute $b^x \pmod{m}$: the result *is* the original message n.

---

3. Euclidean Algorithm.

(a) To find the gcd (greatest common divisor) of two natural numbers a and b:

- **Step 1.** Divide the smaller of these two numbers into the larger.
- **Step 2.** Divide the remainder from the previous step into the divisor from the previous step.
- **Step 3.** Repeat Step 2 until you obtain a remainder of zero.
- **Step 4.** When this happens, the previous remainder **is** $\gcd(a, b)$.

(b) To find integers x and y such that $ax - by = 1$:

- **Step 1.** Take the next-to-last of the "remainder equations" that you produced in finding $\gcd(a, b)$, and solve this equation for its remainder (which, again, is $\gcd(a, b)$).
- **Step 2.** Solve the previous remainder equation for the remainder there, and plug this result into the formula just derived for $\gcd(a, b)$. Then simplify by collecting like terms.
- **Step 3.** Repeat Step 2 until you're done.

---

4. Quantifiers.

(a) The quantifier "$\forall$" means "for all," or "for each," or "for every."
If X is a set and $Q(x)$ is a statement about a quantity x, then the statement

$$\forall x \in X : Q(x)$$

means the statement $Q(x)$ is true for every x in X.

(b) The quantifier "$\exists$" means "for some," or "for at least one," or "there exists."
If X is a set and $Q(x)$ is a statement about a quantity x, then the statement

$$\exists x \in X : Q(x)$$

means the statement $Q(x)$ is true some (at least one, possible more) x in X.

---

5. Counting.

(a) Multiplication principle: if there are m ways of doing Thing 1 and, for each of these ways, there are n ways of doing Thing 2, then there are mn ways of doing Thing 1 and Thing 2 together. Corollary: the number of length-k lists that can be made from n items is

- n^k if repetition is allowed;
- $P(n, k) = n(n-1)(n-2)\cdots(n-k+1) = \dfrac{n!}{(n-k)!}$ if not.

(b) Subtraction principle: the number of lists, or sets, with a property P equals the total number of possible lists, or sets, minus the number of lists, or sets, without property P.

(c) Addition principle: if there are m ways of doing Thing 1 and n ways of doing Thing 2, then there are $m+n$ ways of doing Thing 1 *or* Thing 2 (or both), provided you're not counting twice.

(d) Inclusion-exclusion principle: in general (that is, even if you are counting twice), if there are m ways of doing Thing 1 and n ways of doing Thing 2, then the number of ways of doing Thing 1 *or* Thing 2 (or both) is $m + n$ minus the number of ways of doing Thing 1 *and* Thing 2 together.

(e) The number of k-elements subsets of a set with n elements is

$$C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

---

6. Proof by the principle of mathematical induction.

Theorem. $\forall n \in \mathbb{N},\ A(n)$.

Proof. Step 1: Is $A(1)$ true? [Now do what you need to conclude:] So $A(1)$ is true.

Step 2: Assume $A(k)$. [Now do what you need to conclude:] So $A(k+1)$ follows. So $A(k) \Rightarrow A(k+1)$.

Therefore, by the principle of mathematical induction, $A(n)$ is true $\forall n \in \mathbb{N}$. □

---

7. Basic set definitions. Given sets A and B, and a universe U that contains all sets in question, we define:

(a) $A \cup B = \{x \in U : x \in A \text{ or } x \in B\}$.

(b) $A \cap B = \{x \in U : x \in A \text{ and } x \in B\}$.

(c) $A - B = \{x \in A : x \notin B\}$.

(d) $A \times B = \{\text{ordered pairs } (x, y) : x \in A \text{ and } y \in B\}$.

(e) $\overline{A} = U - A$.

(f) $\mathscr{P}(A) = \{\text{all subsets of } A\}$.

(g) $|P(A)| = 2^{|A|}$ for any set A.

(h) The statement $A \subseteq B$ is equivalent to the statement $x \in A \Rightarrow x \in B$.

---

8. Intersection and union of indexed sets. Given an indexing set I and a set A_α for each $\alpha \in I$, and a universe U, we define

(a) $\bigcup_{\alpha \in I} A_\alpha = \{x \in U : x \in A_\alpha \text{ for some } \alpha \in I\}$.

(b) $\bigcap_{\alpha \in I} A_\alpha = \{x \in U : x \in A_\alpha \text{ for all } \alpha \in I\}$.

---

9. Proof templates.

(a) $P \Rightarrow Q$, direct proof.

Theorem. $P \Rightarrow Q$.
Proof. Assume P. [Now do what you need to conclude:] Therefore, Q.
So $P \Rightarrow Q$. □

(b) $P \Rightarrow Q$, contrapositive proof.

Theorem. $P \Rightarrow Q$.
Proof. Assume $\sim Q$. [Now do what you need to conclude:] Therefore, $\sim P$.
So $P \Rightarrow Q$. □

(c) $P \Leftrightarrow Q$.

Theorem. $P \Leftrightarrow Q$.
Proof. Assume P. [Now do what you need to conclude:] Therefore, Q.
So $P \Rightarrow Q$.
Next, assume Q. [Now do what you need to conclude:] Therefore, P.
So $Q \Rightarrow P$.
Therefore, $P \Leftrightarrow Q$. $\square$

(d) $A \subseteq B$.

Theorem. $A \subseteq B$.
Proof. Assume $x \in A$. [Now do what you need to conclude:] Therefore, $x \in B$.
So $A \subseteq B$. $\square$

(e) $A = B$.

Theorem. $A = B$.
Proof. Assume $x \in A$. [Now do what you need to conclude:] Therefore, $x \in B$.
So $A \subseteq B$.
Now assume $x \in B$. [Now do what you need to conclude:] Therefore, $x \in A$.
So $B \subseteq A$.
Therefore, $A = B$. $\square$

(f) Proof by counterexample. To prove that a statement is false, you need only find one instance where the statement fails.

---

10. Some special sets.

(a) $\mathbb{Z} = \{\text{integers}\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

(b) $\mathbb{N} = \{\text{natural numbers}\} = \{1, 2, 3, \ldots\}$.

(c) $\mathbb{R} = \{\text{real numbers}\} = (-\infty, \infty)$.

(d) $\mathbb{Q} = \{\text{rational numbers}\} = \{\text{fractions } m/n : m, n \in \mathbb{Z} \text{ and } n \neq 0\}$.

(e) Let $a, b \in \mathbb{Z}$. We write $a + b\mathbb{Z}$ for the set $\{a + bm : m \in \mathbb{Z}\}$.

---

11. Facts about integers.

(a) Let $a, b \in \mathbb{Z}$. We say a divides b, written $a|b$, if $b = na$ for some $n \in \mathbb{Z}$.

(b) (Division algorithm.) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

(c) Let $a, b, c \in \mathbb{Z}$. If $c|a$ and $c|b$, then $c|(a + b)$ and $c|(a - b)$.

(d) Let $a, b \in \mathbb{Z}$. If $b|a$, then $b|na$ for any $n \in \mathbb{Z}$.