Puzzle: Caesar cipher

• The Roman dictator Julius Caesar encrypted his personal correspondence using the following code.
  – Number letters of the alphabet: A=0, B=1,... Z=25.
  – To encode a message, replace every letter by a letter three positions before that (wrapping).
    • A letter numbered $x$ by a letter numbered $x-3 \mod 26$.
    • For example, F would be replaced by C, and A by X

• Suppose he sent the following message.
  – QOBXPROB FK QEB ZXSB

• What does it say?
Proof by cases

• Use the tautology $(p_1 \lor p_2) \land (p_1 \rightarrow q) \land (p_2 \rightarrow q) \rightarrow q$
• If $\forall x F(x)$ is $\forall x(G_1(x) \lor G_2(x)) \rightarrow H(x)$,
• prove $(G_1(x) \rightarrow H(x)) \land (G_2(x) \rightarrow H(x))$.
• Proof:
  – Universal instantiation: “let $n$ be an arbitrary element of the domain $S$ of $\forall x$ ”
  – Case 1: $G_1(n) \rightarrow H(n)$
  – Case 2: $G_2(n) \rightarrow H(n)$
  – Therefore, $(G_1(n) \lor G_2(n)) \rightarrow H(n)$,
  – Now use universal generalization to conclude that $\forall x F(x)$ is true.
• This generalizes for any number of cases $k \geq 2$.

$\Box$ (Done).
Proof by cases.

- **Definition** (of odd integers):
  - An integer \( n \) is **odd** iff \( \exists k \in \mathbb{Z}, n = 2 \cdot k + 1 \).

- **Theorem**: Sum of an integer with a consecutive integer is odd.
  - \( \forall x \in \mathbb{Z} \text{ Odd}(x + (x + 1)) \).

- **Proof**:
  - Suppose \( n \) is an arbitrary integer.
  - Case 1: \( n \) is even.
    - So \( n=2k \) for some \( k \) (by definition).
    - Its consecutive integer is \( n+1 = 2k+1 \). Their sum is \( (n+(n+1))= 2k + (2k+1) = 4k+1 \). (axioms).
    - Let \( l = 2k \). Then \( 4k + 1 = 2l + 1 \) is an odd number (by definition). So in this case, \( n+(n+1) \) is odd.
  - Case 2: \( n \) is odd.
    - So \( n=2k+1 \) for some \( k \) (by definition).
    - Its consecutive integer is \( n+1 = 2k+2 \). Their sum is \( (n+(n+1))= (2k+1) + (2k+2) = 2(2k+1)+1 \). (axioms).
    - Let \( l = 2k + 1 \). Then \( n+(n+1) = 2(2k+1)+1= 2l + 1 \), which is an odd number (by definition). So in this case, \( n+(n+1) \) is also odd.
  - Since in both cases \( n+(n+1) \) is odd, it is odd without additional assumptions. Therefore, by universal generalization, get \( \forall x \in \mathbb{Z} \text{ Odd}(x + (x + 1)) \).

\( \Box \) (Done).
Proof by cases

- **Definition**: an absolute value of a real number \( r \) is a non-negative real number \(|r|\) such that if \(|r| = r\) if \( r \geq 0\), and \(|r| = -r\) if \( r < 0\)
  
  - Claim 1: \( \forall x \in \mathbb{R}, |−x| = |x|\)
  - Claim 2: \( \forall x \in \mathbb{R}, −|x| \leq x \leq |x|\)

- **Theorem**: for any two reals, sum of their absolute values is at least the absolute value of their sum.
  
  - \( \forall x, y \in \mathbb{R} |x + y| \leq |x| + |y|\)

- **Proof**:
  
  - Let \( r \) and \( s \) be arbitrary reals. (universal instantiation)
  
  - Case 1: Let \( r + s \geq 0\).
    
    - Then \(|r + s| = r + s\) (definition of \(|\|\))
    - Since \( r \leq |r|\) and \( s \leq |s|\) (claim 2), \( r+s \leq |r| + |s|\) (axioms),
    - so \(|r + s| = r+s \leq |r| + |s|\), which is what we need.
  
  - Case 2: Let \( r + s < 0\).
    
    - Then \(|r + s| = -(r + s) = (-r) + (-s)\) (definition of \(|\|\))
    - Since \(-r \leq |−r| = |r|\) and \(-s \leq |−s| = |s|\) (claims 1 and 2),
    - \(|r+s| = (-r) + (-s) \leq |r| + |s|\) (axioms), which is what we need.
  
  - Since in both cases \(|r+s| \leq |r| + |s|\), and there are no more cases, \(|r+s| \leq |r| + |s|\) without additional assumptions. By universal generalization, can now get \( \forall x, y \in \mathbb{R} |x + y| \leq |x| + |y|\).

\(\square\) (Done).
Square root of 2

• Is it possible to have a Pythagorean triple with \(a=b=1\)?

• Not quite: \(1^2 + 1^2 = 2\), so the third side would have to be \(\sqrt{2}\).

• Is it at least possible to represent \(\sqrt{2}\) as a ratio of two integers?...
  – Pythagoras and others tried...
Proof by contradiction

To prove $\forall x \ F(x)$, prove $\forall x \ \neg F(x) \rightarrow FALSE$

- Universal instantiation: “let $n$ be an arbitrary element of the domain $S$ of $\forall x$ ”
- Suppose that $\neg F(n)$ is true.
- Derive a contradiction.
- Conclude that $F(n)$ is true.
- By universal generalization, $\forall x \ F(x)$ is true.
Rational and irrational numbers

• The numbers that are representable as a fraction of two integers are **rational** numbers. Set of all rational numbers is $\mathbb{Q}$.

• Numbers that are not rational are **irrational**.
  
  – Pythagoras figured out that the diagonal of a square is not comparable to the sides, but did not think of it as a number.
    • More like something weird.
  
  – It seems that irrational numbers started being treated as numbers in 9th century in the Middle East.
    • Starting with a Persian mathematician and astronomer Abu-Abdullah Muhammad ibn Īsa Māhānī (Al-Mahani).

• Rational and irrational numbers together form the set of all real numbers.
  
  – Any sequence of digits, potentially infinite after a decimal point, is a real number. Any point on a line.

• Irrationality of $\sqrt{2}$ is a classic proof by contradiction.
Proof by contradiction

– To prove \( \forall x \ F(x) \), prove \( \forall x \ \neg F(x) \rightarrow FALSE \)

  • Universal instantiation: “let \( n \) be an arbitrary element of the domain \( S \) of \( \forall x \)”
  • Suppose that \( \neg F(n) \) is true.
  • Derive a contradiction.
  • Conclude that \( F(n) \) is true.
  • By universal generalization, \( \forall x \ F(x) \) is true.

\( \square \) (Done).
Definition of rational

• We need a slightly more precise definition of rational numbers for our proof that $\sqrt{2}$ is irrational.

• Definition (of rational and irrational numbers):
  
  – A real number $r$ is rational iff $\exists m, n \in \mathbb{Z}, n \neq 0 \land \gcd(m, n) = 1 \land r = \frac{m}{n}$.

• Reminder: greatest common divisor $\gcd(m,n)$ is the largest integer which divides both $m$ and $n$. When $d=1$, $m$ and $n$ are relatively prime.

• Any fraction can be simplified until the numerator and denominator are relatively prime, so it is not a restriction.

  – A real number which is not rational is called irrational.
Proof by contradiction

• **Theorem**: Square root of 2 is irrational.

• **Proof**:
  
  – Suppose, for the sake of contradiction, that \( \sqrt{2} \) is rational. Then there exist relatively prime \( m, n \in \mathbb{Z} \), \( n \neq 0 \) such that \( \sqrt{2} = \frac{m}{n} \).
  
  – By algebra, squaring both sides we get \( 2 = \frac{m^2}{n^2} \).
  
  – Thus \( m^2 \) is even, and by the theorem we just proved, then \( m \) is even. So \( m = 2k \) for some \( k \).
  
  – \( 2n^2 = 4k^2 \), so \( n^2 = 2k^2 \), and by the same argument \( n \) is even.
  
  – This contradicts our assumption that \( m \) and \( n \) are relatively prime. Therefore, such \( m \) and \( n \) cannot exist, and so \( \sqrt{2} \) is not rational.

\( \square \) (Done).
Puzzle 9

• Susan is 28 years old, single, outspoken, and very bright. She majored in philosophy. As a student she was deeply concerned with issues of discrimination and social justice and also participated in anti-nuke demonstrations.

Please rank the following possibilities by how likely they are. List them from least likely to most likely. Susan is:

1. a kindergarden teacher
2. works in a bookstore and takes yoga classes
3. an active feminist
4. a psychiatric social worker
5. a member of an outdoors club
6. a bank teller
7. an insurance salesperson
8. a bank teller and an active feminist
Set inclusion.

• Let A and B be two sets.
  – Such as A={2,3,4} and B= {1,2,3,4,5}

• A is a **subset** of B:
  – $A \subseteq B$ iff $\forall x \ (x \in A \rightarrow x \in B)$
    • $A \subseteq B$. **FEMINISTS \subseteq PEOPLE**
  – A is a **strict subset** of B: $A \subset B$ iff
    $\forall x \ (x \in A \rightarrow x \in B) \land \exists y \ (y \in B \land y \notin A)$
    • $A \subset B$. **FEMINISTS \subset PEOPLE**
  – When both $A \subseteq B$ and $B \subseteq A$, then $A = B$

• A and B are **disjoint** iff $\forall x \ (x \notin A \lor x \notin B)$
  – {1,5} and {2,3,6,9} are disjoint. So are BANKTELLERS and FEMINISTS in the diagram above.
Operations on sets

- Let A and B be two sets.
  - Such as A={1,2,3} and B={2,3,4}

- **Intersection** \( A \cap B = \{ x \mid x \in A \land x \in B \} \)
  - The green part of the top right picture
  - \( A \cap B = \{2,3\} \)

- **Union** \( A \cup B = \{ x \mid x \in A \lor x \in B \} \)
  - The coloured part in the top picture.
  - \( A \cup B = \{1,2,3,4\} \)

- **Complement** \( \overline{A} = \{ x \in U \mid x \notin A \} \)
  - The blue part on the Venn diagram to the right
  - If universe \( U = \mathbb{N} \), \( \overline{A} = \{ x \in \mathbb{N} \mid x \notin \{1,2,3\} \} \)

- **Difference** \( A - B = \{ x \mid x \in A \land x \notin B \} \)
  - The yellow part in the top picture.
  - \( A - B = \{1\} \)

- **Symmetric Difference** \( A \bigtriangleup B = (A - B) \cup (B - A) \)
  - Both blue parts of the picture to the right.
  - \( A \bigtriangleup B = \{1,4\} \)
Puzzle: the barber

• In a certain village, there is a (male) barber who shaves all and only those men of the village who do not shave themselves.

• **Question: who shaves the barber?**