1. Here is an outline for the formal proof of the divisibility test for 3 which states:

   Theorem 0.1. *3 divides a number if and only if 3 divides the sum of that number's digits*

   Example 0.2.
   3 divides 147012 because
   3 divides $1+4+7+0+1+2=15$

   Example 0.3.
   3 does not divide 37 because
   3 does not divide $3+7=10$

   (a) Prove that if $n|a$ then $n|a+b \Leftrightarrow n|b$
   (b) Write an equation that relates (i) an integer N, and (ii) the sum of N's digits.
   (c) Relate part (a) to finish up your proof.

2. Use Euclid's lemma to prove that if $gcd(m,n)=1$ and $m|a$ and $n|a$ then the product $m \cdot n$ divides a.

3. Prove that if a, b are relatively prime, then $\forall c \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ such that $ax+by=c$.

4. Prove that $gcd(a+3b, b) \leq gcd(a, b+7a)$ for all $a, b \in \mathbb{Z}$ by using the definitions of divisibility and GCD only.

5. Use *proof by induction* to show that $5^{2k}-1$ is divisible by 4 for all $k \in \mathbb{N}$.

6. Let $n \in \mathbb{N}$.

   (a) Use induction to show that exactly one element of the set $\{n, n+1, n+2, n+3\}$ is divisible by 4.
   (b) Use the Division Lemma to show that exactly one element of the set $\{n, n+1, n+2, n+3\}$ is divisible by 4.

7. Let $x \in \mathbb{Z}$.

   (a) Prove that x^2+x is even.
   (b) Prove that $(x^2+x)/2$ is divisible by x if and only if x is odd.
   (c) Prove that $(x^2+x)/2$ is divisible by $x+1$ if and only if x is even.

8. (Houston 26.7 (iii)) Show that if $x^2-3x+2<0$, then $1<x<2$.

9. (Houston 27.23 (v)) Prove that every common divisor of $a, b \in \mathbb{Z}$ is a divisor of $\gcd(a,b)$.

10. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a,b)=1$ and $\gcd(a,c)=1$, then $\gcd(a,bc)=1$.

11. Recall that the Fibonacci numbers are defined by $F_1=1, F_2=1$, and

$$F_{n+1}=F_{n-1}+F_n, \qquad n \geq 2.$$

   (a) Prove that for all $n \in \mathbb{N}$, $\sum_{i=1}^{n} F_n = F_{n+2}-1$.
   (b) Prove that every natural number can be written as the sum of distinct Fibonacci numbers. (This is a harder problem. Hint: use strong induction).

12. Let $a, b, c, d \in \mathbb{Z}$ with a and b nonzero. Prove that if $ab \nmid cd$, then $a \nmid c$ or $b \nmid d$.

13. Let x be an irrational real number. Prove that either x^2 or x^3 is irrational.

14. Prove that for any two sets A and B, $(A \cup B)^c = A^c \cap B^c$.

15. Prove or disprove: For arbitrary k and sets A_i with $i \in \{1, 2, \ldots, k\}$ that $(A_1 \cup A_2 \cup \cdots A_k)^c = A_1^c \cap A_2^c \cdots A_k^c$.

16. Suppose that you own an arbitrarily large amount of 5 cent and 8 cent stamps and none others.

   (a) Show that it is impossible to put 27 cents on an envelope
   (b) Show that it is possible to put every single denomination, 28 cents and higher on an envelope

17. (**Tough**) Show that there exist x, y irrational so that x^y is rational.
    Hint: *Proof by cases*

Exam topics

Methods of Proof

- Direct: $A \Rightarrow B$. Start with hypothesis A, deduce conclusion B.

  Use: Whenever you can. This is the default method.

  Proposition: For integers $a, b, c > 0$, if $a|b$ and $a|c$, then $a|(b+c)$. .
- Cases: $(A \text{ and } C) \Rightarrow B$ and $(A \text{ and not } C) \Rightarrow B$. Assume hypothesis A and take the case where C is true; deduce conclusion B.
  Also, assume A and take the case where C is false; deduce B.

  Use: When you need more information (C or not C) to get from A to B.

  Proposition: For any integer n, we have n^2-n even.
- Contrapositive: not$(B) \Rightarrow$ not(A). Assume B is false, deduce A is false.

  Use: When not(B) is a simpler or more powerful asumption than A.

  Proposition: For $a \in \mathbb{Z}$, if a^2 is even, then a is even.
- Contradiction: $(A \text{ and not } B) \Rightarrow (C \text{ and not } C)$. Assume $A \Rightarrow B$ is false, meaning A is true and B is false. Deduce a contradiction, the impossible statement that C is both true and false.

  Use: As last resort. You can't see why it's true, so you prove it can't be false.

  Proposition: $\sqrt{2}$ is irrational
  To summarize: if you give me a fraction with $\frac{a}{b} = \sqrt{2}$, then I can produce an integer b which is both odd and even.
- Mathematical Induction: To prove $A(n)$ for all integers $n \geq b$:
  Anchor (Base Case) $A(b)$; and Chain Step: for each $n \geq b$, $A(n) \Rightarrow A(n+1)$.

  Use: When the statement $A(n)$ depends on an integer n, and $A(n)$ is part of $A(n+1)$.

  l *Proposition:* For all integers $n \geq 1$, we have $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$.

Axiomatic Systems

- Start with *undefined terms* related to each other by *axioms*, statements assumed true. Make definitions of new terms based on the undefined terms and the axioms.
- Perform proofs within the System, justifying each step by an axiom, a previous result within the System, or a logical prinicple. Logical principles include Methods of Proof, and properties of equality such as: if $a = b$ and $b = c$ then $a = c$.
- *Model:* a way of defining the System's undefined terms as specific objects which satisfy the axioms. Any result proved within the System is valid for all models.
- Example: Group Theory. Starts with an unspecified set G and an unspecified operation $a * b$. Axioms are the most basic desired properties of an operation: closure, associativity, identity element, and inverse elements; not neccesarily commutatitivity.
- Example: Integer Arithmetic. Start with the set $\mathbb{Z}$ and operations $+, \cdot$. Axioms: addition of integers forms a commutative group; multiplication of non-zero integers forms a commutative group except for multiplicative inverses (no reciprocals); multiplication distributes over addition. Also basic properties of inequality $<$, and the validity of Mathematical Induction over positive integers.

Divisibility of integers

- b is a *divisor* (or *factor*) of a, in symbols $b|a$, means $a = bc$ for $c \in \mathbb{Z}$.
- The *greatest common divisor* $d = \gcd(a, b)$ is the largest integer with $d|a$ and $d|b$.
- For $a, b \in \mathbb{Z}$ with $b > 0$, the *division algorithm* gives an integer quotient q and remainder r with: $a = bq + r$ and $0 \leq r < b$.
- The *Euclidean algorithm* for $a > b > 0$ takes successive quotients with remainder: $a = q_1 b + r_1,\ b = q_2 r_1 + r_2,\ r_1 = q_3 r_2 + r_3,\ \ldots,\ r_{k-2} = q_k r_{k-1} + r_k,\ r_{k-1} = q_{k+1} r_k$, so that $a > b > r_1 > \cdots > r_k > 0$.
  - We have $r_k = \gcd(a, b)$.
  - Back-substitution in the algorithm gives integers m, n with $\gcd(a, b) = ma + nb$.
  - We have $d = \gcd(a, b) \iff d|a$ and $d|b$ and $d = ma + nb$ for $m, n \in \mathbb{Z}$.
- Consequences of $\gcd(a, b) = ma + nb$ for $m, n \in \mathbb{Z}$
  - If $e|a$ and $e|b$, then $e|\gcd(a, b)$.
  - Euclid's Lemma: If $a|bc$ and $\gcd(a, c) = 1$, then $a|b$.
  - Prime Lemma: If p is prime with $p|ab$, then $p|a$ or $p|b$.
- A *prime* number is a positive integer p whose only factors are 1 and p itself. A positive integer n which is not prime is *composite*, factoring as $n = ab$ for some $1 < a, b < n$.
- Fundamental Theorem of Arithmetic: Consider an integer $n > 1$.
  - n is a product of primes in a unique way, except for rearrangement of factors.
  - There is a unique list of distinct primes $p_1, \ldots, p_k$ and integer powers $s_1, \ldots, s_k > 0$ with $n = p_1^{s_1} \cdots p_k^{s_k}$.
- Modular arithmetic: Let n be a positive integer, the *modulus*.
  - For $a, b \in \mathbb{Z}$, the relation $a \equiv b \pmod{n}$ means $n \,|\, a-b$.
  - If $a = qn + r$ for $r = 0, 1, \ldots, n-1$, then $n \equiv r \pmod{n}$.
  - If $a \equiv a'$ and $b \equiv b'$, then $a+b \equiv a'+b'$ and $ab \equiv a'b'$.