CONCEPTS OF MATHEMATICS, SUMMER 1 2014
EVEN MORE EXERCISES

Sets, reals, irrationality, etc.

(1) Prove all the facts of real numbers in the notes from the axioms.

(2) Prove the following using only the facts of real numbers in the notes. For a, b, c, d real numbers:
   (a) If a and b are nonzero, $(ab)^{-1} = a^{-1}b^{-1}$.
   (b) If a and b are nonzero, then $(\frac{a}{b})^{-1} = \frac{b}{a}$.
   (c) If b and d are nonzero, then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

(3) A real number x is a *maximal element* (or maximum) of the set X if $x \in X$ and $x \geq y$ for any $y \in X$. Show that any non-empty finite set of reals has a maximal element.

(4) A real number x is an *upper bound* of the set X if $x \geq y$ for any $y \in X$ (but maybe $x \notin X$). x is a *supremum* (or least upper bound) if it is an upper bound and $x \leq y$ for any other upper bound y.

   The completeness axiom of the reals says that any non-empty set X of real numbers which has an upper bound also has a supremum. Use this to show that for any real number x, there exists a natural number n such that $x < n$. *Hint: Otherwise, the set of natural numbers has an upper bound....*

(5) A set of reals is *open* if it is a (maybe infinite) union of open intervals. A set of reals is *closed* if it is a (maybe infinite) intersection of closed intervals. Show that:
   (a) An arbitrary union of open sets is open. An arbitrary intersection of closed sets is closed.
   (b) The intersection of two open sets is open. The union of two closed sets is closed.
   (c) Any finite intersection of open sets is open. Any finite union of closed sets is closed.
   (d) The complement (with respect to $\mathbb{R}$) of an open set is closed, and the complement of a closed set is open.
   (e) $\emptyset$ and $\mathbb{R}$ are both closed and open.
   (f) For real numbers $a < b$, (a, b) is open but not closed, $[a, b]$ is closed but not open.

Date: June 22, 2014.

(g) For real numbers $a < b$, $[a, b)$ and $(a, b]$ are neither open nor closed.

(h) Is an arbitrary union of closed sets necessarily closed? Is an arbitrary intersection of open sets open?

(6) Prove or disprove: Assume A_0, A_1, A_2, ... is a countable family of sets of reals such that for any natural number n, $\bigcap_{i=0}^{n} A_i$ is non-empty. Then $\bigcap_{i=0}^{\infty} A_i$ is non-empty.

(7) What is wrong with the following "proof" that $\sqrt{2}$ is rational?

Let n be the 1000th prime. By the well-ordering principle, there is a minimal natural number m such that $2m^2 = n^2$. Since n is nonzero, m is nonzero, so $2 = \frac{n^2}{m^2}$, or $\sqrt{2} = \frac{n}{m}$.

(8) Assume x and y are rational numbers. Prove that:

(a) $x + y$ is rational.

(b) $-x$ is rational.

(c) xy is rational.

(d) If x is nonzero, x^{-1} is rational.

(9) Assume further that x is positive. Is x^y always rational? Is x^y always irrational?

(10) Assume x is rational but y is irrational. Prove that:

(a) $x + y$ is irrational.

(b) $-y$ is irrational.

(c) If $x \neq 0$, xy is irrational.

(d) y is nonzero and y^{-1} is irrational.

Prove or disprove:

(a) The square root of a rational number is irrational.

(b) The square root of an irrational number is irrational.

(11) For n a negative integer, and x a nonzero real, define x^n by $\frac{1}{x^{-n}}$. Now, for n a nonzero integer and x a non-negative real, define $x^{1/n}$ to be the unique positive y such that $y^n = x$.

(a) Show that y above is indeed unique.

(b) Explain how to extend the definition to x^r for r a rational number and x a positive real.

(c) Show all the usual properties of exponentiation hold for that definition.

Relations, functions

(1) Define a relation E on $\mathbb{Z}$ by aEb if and only if a and b are coprime. Is E an equivalence relation? Which properties of equivalence relations does it satisfy, and which does not it fail to satisfy?

(2) What is wrong with the following "proof" that a relation R on a set A that is symmetric and transitive is also reflexive.

Let $a, b \in A$. We want to show aRa. By symmetry, aRb and bRa, so aRa by transitivity.

(3) Assume $f : \mathbb{R} \to \mathbb{R}$ is a function such that $c := f(1) > 0$ and $f(x + y) = f(x) \cdot f(y)$ for any $x, y \in \mathbb{R}$.
   (a) Show that $f(0) = 1$.
   (b) Show that for any natural number n, $f(n) = c^n$.
   (c) Show that for any rational number r, $f(r) = c^r$.

(4) (a) Is the exponential function $g : \mathbb{N} \to \mathbb{N}$ defined by $g(n) = 2^n$ surjective? Is is injective?
   (b) Is $h : \mathbb{Q} \to \mathbb{Q}$ defined by $h(r) := r^2$ injective? Is is surjective? What if we see it as a function from the positive rationals to the positive rationals?
   (c) Is the relation R on $\mathbb{Q}_{\geq 0}$ defined by xRy if and only if $x = y^2$ a function? What about the same definition but on $\mathbb{R}_{\geq 0}$?

(5) Show that the relation E on the set of functions from $\mathbb{N}$ to $\mathbb{N}$ defined by "fEg if and only if there exists $N \in \mathbb{N}$ such that $f(n) = g(n)$ for all $n \geq N$" is an equivalence relation.

(6) (Hard) Countably many prisoners are in a room. Each is wearing a white or black hat and again each can see the color of the other hats but not the color of her/his own. The prisoners are forbidden to communicate but can discuss a strategy beforehand. The jailers ask the prisoners to simultaneously shout the color of their own hat. Using the previous exercise, show how all but finitely many prisoners can manage to guess correctly. *Hint: The prisoners should first agree on a function F that given a function $f : \mathbb{N} \to \mathbb{N}$ picks out a "canonical" function $g := F(f)$ which is E-equivalent to f. You may take it for granted that there is such a function.*

Cardinalities

(1) Assume A is a finite set and $f : A \to A$. Show that the following are equivalent:
   (a) f is an injection.
   (b) f is a surjection.
   (c) f is a bijection.

Is this also true if A is infinite?

(2) For X a set of real numbers, x is called *X-rational* if it can be written as $\frac{y}{z}$ for $y, z \in X$ and $z \neq 0$. Thus $\mathbb{Q}$ is the set of $\mathbb{Z}$-rational numbers.
   (a) Is a product or a sum of X-rational number X-rational?
   (b) Show that if X is countable, then the set of X-rational numbers is countable.
   (c) Show that if X is countable, there exists real numbers that are not X-rational.

(3) A real number x is called *computable* if there is a computer program (in your favorite language) that given as input a natural number n outputs the nth decimal digit of x. Show that there exists real numbers that are not computable.

Combinatorics

(1) Let B denote the set of bitstrings. For a bitstring s, write $\ell(s)$ for its length, i.e. if s is a binary n-tuple, then $\ell(s) = n$. Let $f : B \to B$ be an injection. Assume that for all $s \in B$, $\ell(f(s)) \leq \ell(s)$. Show that $\ell(f(s)) = \ell(s)$ for all $s \in B$. *Remark: thus there is no perfect compression scheme that compresses some words without also expanding others.*

(2) Assume A, B, and C are finite sets. Give a formula for $|A \cup B \cup C|$ in terms of $|A|$, $|B|$, $|C|$, $|A \cap B|$, $|A \cap C|$, $|B \cap C|$, and $|A \cap B \cap C|$.

(3) After having done the previous question, prove that for any positive natural number n and any finite sets $A_1, A_2, \dots, A_n$:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{S \subseteq [n]} (-1)^{|S|+1} \left|\bigcap_{i \in S} A_i\right|$$

(4) Show that out of $n \geq 1$ real numbers, there is always one which is greater than or equal to their average, and one which is less than or equal to their average.

(5) Assume A is a finite set. How many surjections are there from A to A?

Number theory

(1) Assume p is a prime, $n \geq 2$ is a natural number, and a, b are integers. Assume that p does not divide a, p divides b, but p^2 does not divide b. Show that, $ax^n + b = 0$ has no rational solution.

(2) Use the previous problem to show that for any natural number n, either $\sqrt{n}$ is a natural number, or it is irrational. Conclude that $\sqrt{42}$ is irrational.

(3) Show that if α is irrational, $a, b, a', b' \in \mathbb{Q}$, $a + b\alpha = a' + b'\alpha$, then $a = a'$ and $b = b'$.

(4) Assume α is irrational but α^n is rational for some natural number $n \geq 1$. Let n be minimal with that property. Show that for any natural number m, α^m is irrational if and only if n does not divide m.

(5) Assume n and m are coprime and n is nonzero. Then $\sqrt{\frac{m}{n}}$ is rational if and only if both $\sqrt{n}$ and $\sqrt{m}$ are rational. Explain why we required n and m to be coprime.

(6) Fix a prime p and an integer x such that p does not divide x. Show that the relation E defined on $\mathbb{Z}$ by aEb if and only if for some integer k, $ax^k \equiv b \bmod p$ is an equivalence relation. (For a negative k, we define x^k to be $(x^{-1})^{-k}$, where x^{-1} is an inverse of x modulo p).

(7) Show that a natural number $n \geq 2$ is prime if and only if m does not divide p for all $1 < m \leq \sqrt{n}$.

(8) Assume p is a prime and n is an integer. Show that p and n are coprime if and only if p does not divides n. Conclude that for q a prime, p and q are coprime if and only if $p \neq q$.

(9) Show that the set of prime numbers is countable.

(10) Assume r, k, n, m are integers, n and m are coprime. If r divides kn and r divides km, then r divides k.

(11) Assume k, n, m are integers. If k divides n and m, then k divides $\gcd(n, m)$.

(12) Assume p is prime, x_1, x_2, y_1, y_2 are integers. Assume $x_1 \equiv x_2 \bmod p$, $y_1 \equiv y_2 \bmod p - 1$. Show that $x_1^{y_1} \equiv x_2^{y_2} \bmod p$.

(13) Prove that for every natural number n there is N such that $n \leq \sum_{i=1}^{N} \frac{1}{i}$. *Hint:* $1+1/2+1/3+1/4+1/5+1/6+1/7+1/8 \geq 1 + 1/2 + 1/4 + 1/4 + 1/8 + 1/8 + 1/8 + 1/8\ldots$

(14) Use the above to give another proof that there are infinitely many primes. *Hint: Assume that the set S of primes is finite. Show that there is a constant C such that for any natural number n, $\prod_{p\in S}(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^n}) \leq C$. Then relate $\sum_{i=1}^{N} \frac{1}{i}$ and $\prod_{p\in S}(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^n}))$.*

(15) Assume p is an odd prime and x is an integer. Show that either $x^{(p-1)/2} \equiv 1 \bmod p$, or $x^{(p-1)/2} \equiv -1 \bmod p$.