Quiz Section 4: Number Theory

Review

Divisibility: For $d \neq 0$ we write $(d \mid a)$ iff there is an integer k such that $a = kd$.
Division Theorem: For integers a and b with $b > 0$, there are unique integers q and r such that $a = qb + r$ and $0 \leqslant r < b$. The remainder r is also written as $a \bmod b$.
Mod Predicate $(\bmod m)$: For integer $m > 0$ and integers a and b, we write $a \equiv_m b$ iff $m|(a - b)$. This is equivalent to $(a - b) = km$ for some integer k; it is also equivalent to $a = b + km$ for some integer k.
Properties of $(\bmod m)$:

- For $m > 0$, $a \equiv_m b$ iff $a \bmod = b \bmod m$.
- If $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.
- If $a \equiv_m b$ and $c \equiv_m d$ then
  - $a + c \equiv_m b + d$
  - $ac \equiv_m bd$

Prime: An integer $n > 1$ is prime iff its only positive divisors are 1 and n.
Unique Factorization Theorem: Every positive integer has a unique representation as a product of prime numbers (assuming that the primes in the product are listed with smaller ones first).
Greatest Common Divisor: $gcd(a, b)$ is the largest common divisor of a and b.
Properties of gcd: For positive integers a and b, $gcd(a, 0) = a$ and $gcd(a, b) = gcd(b, a \bmod b)$.
Multiplicative Inverse: For $m > 0$ and $0 \leqslant a < m$, the *multiplicative inverse of a modulo m* is a number b with $0 \leqslant b < m$ such that $ab \equiv_m 1$. It exists if and only if $gcd(a, m) = 1$.

Task 1 – Even / Odd

For any predicate for which we have a definition, we have rules that allow us to replace the predicate with its definition or vice versa. As an example, consider "Even", defined by $\text{Even}(x) := \exists y\,(x = 2 \cdot y)$ for the domain of integers. We can use this definition via these two rules:

Def of Even

$$\frac{\text{Even}(x)}{\therefore\ \exists y\,(x = 2 \cdot y)}$$

Undef Even

$$\frac{\exists y\,(x = 2 \cdot y)}{\therefore\ \text{Even}(x)}$$

For example, if we know $\text{Even}(6)$ holds, then "Def of Even" allows us to infer $\exists y\,(6 = 2 \cdot y)$. On the other hand, if we know that $\exists y\,(10 = 2 \cdot y)$, then "Undef Even" allows us to infer $\text{Even}(10)$. In English proofs, we do not distinguish between replacing $\text{Even}(x)$ by its definition and vice versa (both are "by the definition of Even").

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall x\,\forall y\,((\text{Even}(x) \wedge \text{Odd}(y)) \rightarrow \text{Odd}(x + y))$$

In English, this says that, for any even integer x and odd integer y, the integer $x + y$ is odd.

a) Write a **formal proof** that the claim holds.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 2 – Division of Labor

In this problem, we will use the predicate "Divides", defined by $\text{Divides}(x, y) := \exists k\,(y = k \cdot x)$. We can use this definition via these two rules:

Def of Divides

$$\frac{\text{Divides}(x, y)}{\therefore\ \exists k\,(y = k \cdot x)}$$

Undef Divides

$$\frac{\exists k\,(y = k \cdot x)}{\therefore\ \text{Divides}(x, y)}$$

Note that, in math, we write Divides(x, y) with the nicer notation "$x \mid y$".

Let domain of discourse be the integers. Consider the following claim: $\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$. In English, this says that if an integer b divides an integer a, then the square of b will divide the cube of a.

a) Write a **formal proof** that the claim holds.

b) Translate your formal proof to an **English proof**.
Note: Keep in mind that your English proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 3 – Congruent

Write a formal proof of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. Then, translate it into an English proof.

Task 4 – Divide Both Sides

For any known theorem, we have rules that allow us to cite the fact that the theorem holds and, if the statement of the theorem is a domain-restricted $\forall$, to apply it in one step to specific values.

In this problem, we will use the theorem "DivideEqn". It says that, if you have the equation $ca = cb$ and you know that $c \neq 0$, then you can divide both sides of the equation by c to get $a = b$. We can use this theorem in a formal proof via these two rules:

Cite DivideEqn

$$\therefore \quad \forall a \, \forall b \, \forall c \, ((ca = cb \wedge \neg(c = 0)) \rightarrow a = b)$$

Apply DivideEqn

$$\frac{ca = cb \wedge \neg(c = 0)}{\therefore \quad a = b}$$

The first rule simply writes down the statement of DivideEqn. To use it, you apply Elim $\forall$ to get an implication and then Modus Ponens to get the conclusion. The second rule does these three things (Cite, Elim $\forall$, Modus Ponens) in a single step.

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

In English, this says that, for any integers a, b, and m, if $5a$ is congruent to $5b$ modulo $5m$, then a is congruent to b modulo m.

a) Write a **formal proof** on cozy that the claim holds. You are given the facts $5 \neq 0$, so that you may divide by 5. Use the link `https://tinyurl.com/sec4task4`

We **strongly** recommend that you use the first rule above, via "`cite DivideEqn`" in Cozy. If you want try using the second rule, you will need to consult the Cozy documentation.

Note that this theorem only applies to an equation that looks like $c(\dots) = c(\dots)$ for some c. If your equation doesn't look exactly like this, then you would need to use Algebra to first put it in this form. For example, if your equation says $ca + cb = 5c$, then you would need to rewrite it as $c(a + b) = c(5)$ with Algebra before applying DivideEqn.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 5 – This is Really Mod

Let n and m be integers greater than 1, and suppose that $n \mid m$. Give an English proof that for any integers a and b, If $a \equiv_m b$ and $m \equiv_n 0$, then $a \equiv_n b$.

Task 6 – Theorem

Let the domain of discourse be the integers. Consider the following claim:

$$\forall\, n, \texttt{Odd}\, n \vee \texttt{Even}\, n$$

In English, this says that every integer n is either even or odd.

In this problem, we will use the Division theorem. It says that for $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$, there exist unique integers q, r with $0 \leqslant r < d$, such that $a = dq + r$. We will also provide you with a Lemma that says, if $0 \leqslant r < 2$, then $r = 0$ or $r = 1$.

Cite DivisionEqn

$$\therefore \quad \forall a\, \forall b\, ((d > 0) \to \exists\, r, \exists\, q(0 \leqslant r < d \wedge a = dq + r))$$

Lemma 1

$$0 \leqslant r < 2$$
$$\therefore \quad r = 0 \vee r = 1$$

a) Write a **formal proof** that the claim holds.

b) Translate your formal proof to an **English proof**.