Math 2710 (Roby) **Practice Midterm #1** Spring 2013

1. Use a truth table to check whether the statement $(P \text{ AND } Q) \implies R$ is equivalent to the statement $P \implies (Q \implies R)$.

   A complete truth table looks as follows.

P	Q	R	P AND Q	$Q \implies R$	$(P \text{ AND } Q) \implies R$	$P \implies (Q \implies R)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	F	F	T	T	T
T	F	F	F	T	T	T
F	T	T	F	T	T	T
F	T	F	F	F	T	T
F	F	T	F	T	T	T
F	F	F	F	T	T	T

   Comparing the last two columns, we see that the statements have the same truth value in each row, so they are equivalent. Another way to see this would be to note that an implication can be *False* if and only if is hypothesis is true and its conclusion is false. For the first statement, this happens exactly when R is false, and P AND Q is true, i.e, (P, Q, R) is (T, T, F). For the second, we need P true, and $Q \implies R$ false, but the latter only happens when Q is true and R is false, i.e., (P, Q, R) is (T, T, F).

2. **PODASIP:** For all integers $a, b \in \mathbb{Z}$, $a \mid b \implies a \leq b$.

   This is *false*. A counterexample is $3 \mid -6$, but $3 > -6$.

   SALVAGE: True if $a, b > 0$.

   Proof. By definition of divisibility, $\exists\, k \in \mathbb{Z}$ such that $b = ak$. Now, $a, b > 0 \implies k > 0$ (which we haven't learned to prove carefully yet, but you can assume this). Since there are no integers between 0 and 1, we get that $1 \leq k \implies a \leq ak = b$ (since $a > 0$ and multiplying an inequality by a positive number keeps the sign, another fact we haven't proved carefully yet). ■

3. **PODASIP:** For any sets S and T: $(S \cap T = \emptyset)$ AND $(S \cup T = T) \implies S = \emptyset$.

   Proof. Suppose BWOC that $S \neq \emptyset$. Let $x \in S$. Since $S \cap T = \emptyset$, this means $x \notin T$. But then $x \in S \cup T \implies x \in T$, contradiction. Hence, our supposition is false, and $S = \emptyset$. ■

4. For each linear diophantine equation below, do the following:

   (a) Determine whether it has a solution in $\mathbb{Z}^2$.

   (b) Find one solution.

(c) Describe the set of all solutions;

(d) Describe all solutions in *positive* integers.

$$18x + 5y = 48 \tag{1}$$
$$14x + 35y = 93 \tag{2}$$

For (1) we note that $\gcd(18, 5) = 1$ which divides 48, so there is a solution. One can be found using Euclid's algorithm and the magic box or back substitution to get $(2, -7)$ is a solution to LHS=1. Multiply by 48 to get the solution $(96, -336)$ to (1). Now the general solution is given by

$$x = 5t + 96 \quad \text{and} \quad y = -18t - 336 \quad \forall\, t \in \mathbb{Z}\,.$$

If we want solutions in *positive* integers, then we the expressions in t above to simultaneously be positive, i.e.,

$$5t + 96 > 0 \implies t > -19.2$$
$$-18t - 336 > 0 \implies t < -18\frac{2}{3}$$

so the only possibility is $t = -19$, which gives the solution $(1, 6)$.

For (2) simply note that $\gcd(14, 35) = 7$, which does not divide 93, so there can be no integer solutions at all.

5. Show that there are infinitely many primes in $\mathbb{Z}$ of the form $4k + 3$.

Proof. Notice first that the product of two numbers of the form $4k + 1$ is of the same form, since

$$(4k + 1)(4\ell + 1) = 16k\ell + 4k + 4\ell + 1 = 4(4k\ell + k + \ell) + 1$$

Now suppose BWOC that we had only finitely many primes in $\mathbb{Z}$ of the form $4k + 3$, call them $q_1, q_2, \ldots q_r$. Define

$$N = 4q_1 \cdots q_r - 1$$

When we divide N by any of the q_i, we get a remainder of $q_i - 1$, so none of them are a factor. Since N is odd, all of its prime factors must be odd, so they all must be of the form $4k + 1$. But then their product would be of the form $4k + 1$, while N is of the form $4k + 3$, contradiction. Hence, there are infinitely many primes of the form $4k + 3$. ∎

6. Describe the chain of reasoning that takes one from basic properties of $\mathbb{Z}$ to the Fundamental Theorem of Arithmetic (aka, Unique Factorization Theorem).

   From the basic properties of $\mathbb{Z}$ we can show that we have division (with remainder), which we iterate to get Euclid's algorithm. This must terminate by the well-ordering principle, since the remainders strictly decrease. Applying this algorithm to $a, b \in \mathbb{Z}$, allows us to construct solutions to the diophantine equation $ax + by = \gcd(a, b)$. From this we get Euclid's Lemma, that $p \mid ab \implies p \mid a$ or $p \mid b$ when p is *prime*. Showing that every integer n has some factorization is elementary, and showing uniqueness follows from Euclid's Lemma and a strong induction argument.

7. **True/False & Explain:** For each statement below, state whether it is true or false and give a convincing reason.

   (a) $\forall x, y \in \mathbb{Q}\,,\ \exists z \in \mathbb{Q}$ s.t. $x < z < y$.

   True, since we could take $z = \frac{x+y}{2}$. This property of $\mathbb{Q}$ is described as "$\mathbb{Q}$ is a dense subset of itself".

   (b) $\exists z \in \mathbb{Q}$ s.t. $\forall x, y \in \mathbb{Q}\,,\ x < z < y$

   False. This statement says that we can find a *single* $z \in \mathbb{Q}$ which is between *every* pair of rational numbers. But once I've picked z, I can't change it later, and then $x = z - 1$ and $y = z - 2$ would be elements of $\mathbb{Q}$ which are both smaller than z.

   (c) $\exists y \in \mathbb{Z}$ s.t. $x + y = x\ \forall x \in \mathbb{Z}$.

   True, namely the additive identity $y = 0 \in \mathbb{Z}$.

   (d) $\exists y \in \mathbb{Z}$ s.t. $\forall x \in \mathbb{Z}\,,\ x + y = 0$.

   False. This statement says that we can find a *single* $y \in \mathbb{Z}$ which is an additive inverse to *every* $x \in \mathbb{Z}$. Once we've picked y, then let $x = -y + 1$, which will give $x + y = 1$, not 0.

8. Explain what is wrong with the following proof attempt:

   > *We want to show that* $a \mid b$ AND $b \mid c \implies a \mid c$. *Suppose by way of contradiction that the statement was false, so* $a|b$ *and* $b|c$, *but* $a \nmid b$. *But we see immediately that* $3 \mid 6$ *and* $6 \mid 12$, *while* $3 \mid 12$, ***contradiction***. *Therefore, the original statement must be true.* ∎

   In a proof by contradiction, one supposes (BWOC) the statement is false (i.e., the conclusion is false and the hypotheses are true) and reaches a contradiction with something that is already known, e.g., a previously proven result, or a basic axiom. Having made the supposition, one is no longer allowed to use counterexamples. Notice that the counterexample is essentially just a single example that the statement is true, which could never be sufficient to establish its general truth.