Homework #3: Predicate Logic, and Number Theory
Due Date: October 13, 2005
Student: Jan Voung (jvoung@cs.ucsd.edu)

Predicate Logic

Solutions to LO $\{2.6, 2.18, 2.19, 2.20, \text{Review } 7, \text{ and } 9\}$ are in the book.

Notes:

- 2.19 - The counter-example for (b), and (c) are slightly reversed. Let $D = \mathbb{Z}$, let $P(x)$ be "x is even" and let $Q(x)$ be "x is odd". For (b), the second statement ($\exists x \in \mathbb{Z}$, "x is even") $\wedge$ ($\exists x \in \mathbb{Z}$, "x is odd") is true, but the first statement $\exists x \in \mathbb{Z}$, "x is odd" $\wedge$ "x is even" is false.

- 2.20 - In more detail:

  Let $n = ab$, where $a, b > 1$ since n is composite. A useful equation is:

  $$\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$$

  Applying this to $r = 2$ we get

  $$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{n-1} &= \sum_{i=0}^{n-1} 2^i \\ &= \frac{1-2^n}{1-2} \\ &= \frac{1-2^n}{-1} \\ &= 2^n - 1 \end{aligned}$$

  Since we want to show $2^n - 1$ is composite, the summation could come in handy. If we can factor $2^n - 1 = cd$, then it is composite. Perhaps selectively summing some of the terms will be equivalent to factoring. Since $n = ab$ is already factored, maybe sum terms with an exponent a multiple of a or b:

  $$2^{0 \cdot a} + 2^{1 \cdot a} + \ldots + 2^{k \cdot a}$$

We don't want can $k \cdot a$ to exceed $n-1$ so:

$$\begin{aligned} k \cdot a &\leq n-1 \\ k &\leq \frac{n}{a} - \frac{1}{a} \\ k &\leq b - \frac{1}{a} \\ k &\leq b-1 \end{aligned}$$

The last step is to ensure k is an integer. Back to the summation:

$$\begin{aligned} 2^{0\cdot a} + 2^{1\cdot a} + \ldots + 2^{(b-1)\cdot a} &= \sum_{i=0}^{b-1} (2^a)^i \\ &= \frac{1-(2^a)^b}{1-(2^a)} \\ &= \frac{1-2^n}{1-2^a} \\ &= \frac{2^n-1}{2^a-1} \end{aligned}$$

Let $c = \frac{2^n-1}{2^a-1}$ and $d = 2^a - 1$. Then

$$c \cdot d = \frac{2^n-1}{2^a-1} \cdot (2^a-1) = 2^n - 1$$

and we have factored $2^n - 1$. This is valid because c and d are both integers > 1. c represents the sum $2^{0\cdot a} + 2^{1\cdot a} + \ldots + 2^{(b-1)\cdot a}$ of integers. This makes c an integer > 1. Also, since a is an integer > 1, $d = 2^a - 1$ is an integer > 1.

- Answers to review questions 7 and 9 are after all the questions.

Number Theory

Solutions to NT $\{1.3, 1.8, 1.11, 1.17\}$ are in the book.

Notes:

- A good way to prove "if and only if" statements is to prove the "if" part separately from the "only if" part. Let's look at 1.3(a) for example.

  Prove: The product of two integers is even if and only if at least one of them is even.

$\Rightarrow$ (the "if" part): Assume the product of two integers $x \cdot y$ is even (this is actually a given for the "if" part). So $x \cdot y = 0 \mod 2$. For the sake of contradiction, assume both numbers are odd. That is, $x = 1 \mod 2$ and $y = 1 \mod 2$. Then $x \cdot y = 1 \mod 2$, a contradiction. Therefore, at least one of x, y must be even.

$\Leftarrow$ (the "only if" part): You no longer assume that the product xy is even. That is what you must show now. However, you are now given that at least one of the integers is even. Without loss of generality say x is even (otherwise, relabel the two). So $x = 0 \mod 2$. Well, 0 times anything is $0 \mod 2$. Therefore, $xy = 0 \mod 2$, meaning the product is even.