Problem Set 4

Engineering 3422, 2005

To do for Oct 13th.

Q0. Prove that

$$NotThenDFF(x,y) \Leftrightarrow DFFThenNot(x,y)$$

where

$$\begin{aligned}
NotThenDFF(x,y) &\triangleq \exists z, Not(x,z) \wedge DFF(z,y) \\
DFFThenNot(x,y) &\triangleq \exists z, DFF(x,z) \wedge Not(z,y) \\
Not(x,y) &\triangleq (\forall t, y(t) \leftrightarrow \neg x(t)) \\
DFF(x,y) &\triangleq (\forall t, y(t+1) \leftrightarrow x(t))
\end{aligned}$$

In each case t ranges over $\mathbb{N}$ and x, y, and z range over functions from $\mathbb{N}$ to $\{T, F\}$.

Q1. Prove the following conjectures or find counter-examples

Conjecture: For all $a, b, c, k \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$ then

- $a \mid b + c$
- $a \mid k \cdot b$
- $a \mid b - c$

Conjecture: For all $a, b, c \in \mathbb{N}$,

- Reflexivity: $a \mid a$
- Antisymmetry: If $a \mid b$ and $b \mid a$ then $a = b$
- Transitivity: If $a \mid b$ and $b \mid c$ then $a \mid b$.

Conjecture: For all $a, b, c, d \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

- $ac \equiv bd \pmod{m}$

Theorem: For all integers a and b,

- $\gcd(0, b) = b$, where b is a positive integer.

- $\gcd(a, b) = \gcd(b, a)$

Q2. Is the following a theorem? If so prove it; if not find a counter-example.
Conjecture: For all $a, b \in \mathbb{N}$,

- If $a \mid b$ then $a \leq b$.

Q3. Use proof by contradiction to show that, for any sets A, B

$$(A - B) \cap B = \emptyset$$

Q4. (a) Here is a table of $a^i \bmod 3$ for $i \in \{0, 1, 2\}$ and $a \in \{1, 2, ..., 6\}$.

$a^i \bmod 3$	$i =$ 0	1	2	3	4	5	6
$a = 1$	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1

Make a table of $a^i \bmod 5$ for $i \in \{0, 1, ..., 4\}$ and $a \in \{1, 2, ...4\}$. Do the same for $a^i \bmod 7$ for $i \in \{0, 1, ..., 6\}$ amd $a \in \{1, 2, ..., 6\}$. Make a similar table for $a^i \bmod 11$. What does this suggest about $a^{p-1} \bmod p$ for prime numbers p and $0 < a < p$?

(b) Bonus. Circle any repeating cycles Can you show that the cycles in such a table will always be of a length that divides $p - 1$? Hint, show that for each cycle you can make a rectangle that has the cycle as its first line and that is filled with all the numbers from1 to $p - 1$ each once.Here is one such rectangle for $p = 11$, $a = 3$

1	3	9	5	4
2	6	7	10	8

(c) From the result in **(b)**, can you prove your conjecture from part **(a)**?

If you make the right conjecture in part (a) and complete (b) and (c) you have just proved Fermat's little theorem.