Analysis and Verification of Software
Homework 4

due by March 17, 2015
The congruence domain consists of abstract values denoted, $a\mathbb{Z} + b$, Where $b \in \mathbb{Z}$ and $a \in \mathbb{N}$. We will call $a$ the modulo and $b$ the remainder.

The lattice operators $\sqcup$ and $\sqcap$ are defined as follows (due to [Gra89]).

\[
(a\mathbb{Z} + b) \sqcup (a'\mathbb{Z} + b') = \gcd\{a, a', |b - b'|\}\mathbb{Z} + \min\{b, b'\}
\]

\[
(a\mathbb{Z} + b) \sqcap (a'\mathbb{Z} + b') = \text{lcm}\{a, a'\}\mathbb{Z} + b'' \text{ if } b \equiv b' \mod \gcd\{a, a'\}
\]

\[
(a\mathbb{Z} + b) \sqcap (a'\mathbb{Z} + b') = \bot \text{ otherwise.}
\]

where \(b'' \equiv b \mod a\) and \(b'' \equiv b' \mod a'\). Other cases follows from the lattice axioms.

The abstraction and concretization maps for this domain are defined as follows:

\[\alpha\{\{n\}\} = 0\mathbb{Z} + n\]

\[\alpha(M) = \gcd\{|b - b'| | b, b' \in M\}\mathbb{Z} + \min\{b | b \in M\}\]

\[\gamma(a\mathbb{Z} + b) = \{an + b | \forall n \in \mathbb{Z}\}\]

\[\gamma(\top) = 1\mathbb{Z} + 0 = \mathbb{Z}\]

\[\gamma(\bot) = \emptyset\]

In words the set $\gamma(a\mathbb{Z} + b)$ contains all integers that are congruent to $b$ modulo $a$. 
Examples

• The element \((2\mathbb{Z} +1)\) represents the odd integers:
  \[-7, -5, -3, -1, 1, 3, 5, 7,\ldots\]
• The element \((3\mathbb{Z} +2)\) represents the integers:
  \[-4, -1, 2, 5, 8, 11, 14,\ldots\]
• The element \((5\mathbb{Z} +0)\) represents the integers:
  \[-15, -10, -5, 0, 5, 10, 15, 20,\ldots\]
The basic operators on the congruence domain are defined in the table below:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Congruence</th>
</tr>
</thead>
<tbody>
<tr>
<td>∪</td>
<td>$(a\mathbb{Z} + b) \sqcup (a'\mathbb{Z} + b') = \gcd{a, a', b - b'}\mathbb{Z} + \min(b, b')$</td>
</tr>
<tr>
<td>∩</td>
<td>$(a\mathbb{Z} + b) \cap (a'\mathbb{Z} + b') = \text{cond}(b \equiv b' \mod \gcd(a, a'), \text{lcm}(a, a')\mathbb{Z} + b'', \bot)$</td>
</tr>
<tr>
<td>⊆</td>
<td>$(a\mathbb{Z} + b) \subseteq (a'\mathbb{Z} + b') \iff a'</td>
</tr>
<tr>
<td>⊕</td>
<td>$(a\mathbb{Z} + b) \oplus (a'\mathbb{Z} + b') = \gcd(a, a')\mathbb{Z} + (b + b')$</td>
</tr>
</tbody>
</table>

Elements

| ⊤         | $\mathbb{Z}$ (that is, $a = 1, b = 0$) |
| ⊥         | $\emptyset$ |

Galois connection

| $\alpha$  | $\alpha(k) = 0\mathbb{Z} + k$ |
| $\gamma$  | $\gamma(a\mathbb{Z} + b) = \{ak + b | k \in \mathbb{Z}\}$ if $a \neq 0$ |
|           | $\gamma(a\mathbb{Z} + b) = \{b\}$ if $a = 0$ |

Let $a\mathbb{Z} + b$ and $a'\mathbb{Z} + b'$ be two non-bottom abstract values. Then

$$(a\mathbb{Z} + b)(a'\mathbb{Z} + b') = \gcd\{aa', ab', a'b\}\mathbb{Z} + bb'$$

is a correct approximation of multiplication.
Exercise 1

• Depict the Venn diagram of the congruence domain. Its elements are \((a\mathbb{Z}+b)\) where if \(a \neq 0\), then \(b < a\). (of course, as it is an infinite domain, you can just represent a part of it!)

• For each operation (sum, difference, multiplication, lub, and glb) discuss the result of the application of the definition above to the case \((13\mathbb{Z} + 5)\) and \((5\mathbb{Z} + 2)\)
Exercise 2

• Is the domain of congruences a complete lattice?

If your answer is YES, prove it!
If your answer is NO, show a counterexample!
Exercise 3

• Does the domain of congruences satisfy the ascending chain condition ACC?

If your answer is YES, prove it!
If your answer is NO, show a counterexample!
Exercise 4

• Consider the following program:

\[
f(x) = \begin{cases} 
  y = 1 \\
  \text{while } (x > 0) \{ \\
  \quad y = x \times y \\
  \quad x = x - 1 \\
  \} 
\end{cases}
\]

• Compute the concrete semantics of this program, and its abstract semantics on the congruence domain.