Solution of CSE20 Exercise 2

February 16, 2010

Question 1

Represent 38 with a residual number system of moduli $(m_1, m_2, m_3) = (3, 5, 7)$.

$$(38\%3, 38\%5, 38\%7) = (2, 3, 3)$$

Question 2

Suppose $(x\%5, x\%7, x\%11) = (1, 2, 3)$. Find the smallest positive integer x that satisfies this system.

We use the Chinese remainder theorem. Recall that

$$x \equiv \sum_{i=1}^{k} M_i s_i r_i \pmod{M}$$

where

$$M = \prod_{i=1}^{k} m_i,$$

$$M_i = \frac{M}{m_i},$$

and s_i is the unique value mod m_i such that

$$M_i s_i \equiv 1 \pmod{m_i}.$$

Plugging in our values, we have

$$\begin{array}{rcll} M &=& 5 \cdot 7 \cdot 11 & = 385 \\ M_1 &=& 7 \cdot 11 & = 77 \\ M_2 &=& 5 \cdot 11 & = 55 \\ M_3 &=& 5 \cdot 7 & = 35 \end{array}$$

We now solve for each of the s_i. We need

$$M_1 s_1 \equiv 1 \pmod{5}$$

or

$$77 s_1 \equiv 1 \pmod{5},$$

which is satisfied by $s_1 = 3$. We need

$$M_2 s_2 \equiv 1 \pmod{7}$$

or

$$55 s_2 \equiv 1 \pmod{7},$$

which is satisfied by $s_2 = 6$. Finally, we need

$$M_3 s_3 \equiv 1 \pmod{11}$$

or

$$35 s_3 \equiv 1 \pmod{11},$$

which is satisfied by $s_3 = 6$.

Now we plug all our values into the expression from the Chinese remainder theorem.

$$\begin{aligned}
x &\equiv \textstyle\sum_{i=1}^{k} M_i s_i r_i \pmod{M} \\
&\equiv \textstyle\sum_{i=1}^{3} M_i s_i r_i \pmod{M} \\
&\equiv 77 \cdot 3 \cdot 1 + 55 \cdot 6 \cdot 2 + 35 \cdot 6 \cdot 3 \pmod{385} \\
&\equiv 231 + 660 + 630 \pmod{385} \\
&\equiv (231\%385) + (660\%385) + (630\%385) \pmod{385} \\
&\equiv 231 + 275 + 245 \pmod{385} \\
&\equiv 366 \pmod{385}
\end{aligned}$$

So the smallest positive number that satisfies this system is 366.

Question 3

Show the operation of 38+44 in a residual number system with moduli $(m_1, m_2, m_3) = (3, 5, 7)$.

From question 1, we have 38 is $(2, 3, 3)$ in this system. We represent 44 by

$$(44\%3, 44\%5, 44\%7) = (2, 4, 2).$$

Adding our representations pairwise and modding appropriately, we get

$$\begin{aligned}
(2 + 2\%3, 3 + 4\%5, 3 + 2\%7) &= (4\%3, 7\%5, 5\%7) \\
&= (1, 2, 5)
\end{aligned}$$

Question 4

Show the operation of 19×15 in a residual number system with moduli $(m_1, m_2, m_3) = (5, 13, 14)$.

We represent 19 in this system by

$$(19\%5, 19\%13, 19\%14) = (4, 6, 5).$$

We represent 15 in this system by

$$(15\%5, 15\%13, 15\%14) = (0, 2, 1).$$

Finally, we multiply pairwise and mod appropriately:

$$\begin{array}{rcl} (4 \times 0\%5, 6 \times 2\%13, 5 \times 1\%14) & = & (0\%5, 12\%13, 5\%14) \\ & = & (0, 12, 5) \end{array}$$

Question 5

Residual Number System: State and prove the Chinese remainder theorem.

Please refer to lecture notes.

Question 6

Prove that for any a and b in the set B of a Boolean algebra, $(a+b)(a+b') = a$.

$$\begin{array}{rcll} (a+b)(a+b') & = & a + bb' & \text{Distributivity} \\ & = & a + 0 & \text{Definition of Complement} \\ & = & a & \text{0 is identity for } + \end{array}$$

Question 7

Prove general associativity holds for $+$ in any Boolean algebra: For all $n \geq 1$,

$$a_1 + (a_2 + (a_3 + (\ldots + a_n))) = (((a_1 + a_2) + a_3) + \ldots) + a_n$$

You may assume that associativity holds for $n = 3$.

The proof is by induction on n.

It clearly holds for the case where $n = 1$: $a_1 = a_1$.

It also clearly holds when $n = 2$: $a_1 + a_2 = a_1 + a_2$.

We're allowed to assume it for $n = 3$: $a_1 + (a_2 + a_3) = (a_1 + a_2) + a_3$.

Now suppose $n > 3$. We are allowed to assume:

$$a_1 + (a_2 + (a_3 + (\ldots + a_k))) = (((a_1 + a_2) + a_3) + \ldots) + a_k$$

for all $k < n$. We must show:

$$a_1 + (a_2 + (a_3 + (\ldots + a_n))) = (((a_1 + a_2) + a_3) + \ldots) + a_n$$

We proceed by use of the induction hypotheses, which allow use to rearrange subterms of the left-hand-side:

$$\begin{array}{lll} & a_1 + (a_2 + (a_3 + (\ldots + a_n))) & \\ = & a_1 + (((a_2 + a_3) + \ldots) + a_n) & \text{Inductive Hypothesis for } n-1 \\ = & (a_1 + ((a_2 + a_3) + \ldots)) + a_n & \text{Inductive Hypothesis for } n=3 \\ = & (a_1 + (a_2 + (a_3 + \ldots)) + a_n & \text{Inductive Hypothesis for } n-2 \\ = & (((a_1 + a_2) + a_3) + \ldots) + a_n & \text{Inductive Hypothesis for } n-1 \end{array}$$

Question 8

Boolean Algebra: State and prove De Morgan's laws.

Please refer to lecture notes.

Question 9

Show the operation tables for a Boolean algebra of four elements.

Let's have our set $B = \{0, 1, 2, 3\}$. Let's begin with empty tables for our operators, + and *:

+	0	1	2	3
0				
1				
2				
3				

$*$	0	1	2	3
0				
1				
2				
3				

Let's pick the identity for + to be 0. By the identity postulate, we must have $a + 0 = a$ for any a, and also that $0 + a = a$ by commutativity. We fill in the + table accordingly:

+	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

Similarly, we pick the identity for $*$ to be 3. By the identity postulate, we have $a * 3 = a$, and by commutativity we also have $3 * a = a$. We fill in the $*$

table accordingly:

$*$	0	1	2	3
0				0
1				1
2				2
3	0	1	2	3

We can also derive the boundedness laws, which say $a + 3 = 3$ and $a * 0 = 0$ (and, by commutativity, $3 + a = 3$ and $0 * a = 0$). We add the implied entries to the tables:

$+$	0	1	2	3
0	0	1	2	3
1	1			3
2	2			3
3	3	3	3	3

$*$	0	1	2	3
0	0	0	0	0
1	0			1
2	0			2
3	0	1	2	3

We can also derive the idempotency laws: $a + a = a$ and $a * a = a$. So we add the entries implied by this as well:

$+$	0	1	2	3
0	0	1	2	3
1	1	1		3
2	2		2	3
3	3	3	3	3

$*$	0	1	2	3
0	0	0	0	0
1	0	1		1
2	0		2	2
3	0	1	2	3

Now we're left with only the entries for $2+1$, $1+2$, $1*2$, and $2*1$. Clearly the entries for $1+2$ and $2+1$ must be the same by commutativity; the same is true of $1*2$ and $2*1$. We notice also that 1 and 2 don't have complements. Also, 0 and 3 are complements of each other. Because complements are unique, 0 and 3 cannot be complements of 1 and 2; 1 and 2 must be complements of each other. So $1 + 2 = 2 + 1 = 3$ and $1 * 2 = 2 * 1 = 0$ by the complement postulate:

$+$	0	1	2	3
0	0	1	2	3
1	1	1	3	3
2	2	3	2	3
3	3	3	3	3

$*$	0	1	2	3
0	0	0	0	0
1	0	1	0	1
2	0	0	2	2
3	0	1	2	3

It remains to prove that these operations are distributive.

Question 10

Simplify formula $(pq + r')(p + r)(q + r)$

$$\begin{array}{rcll} (pq + r')(p + r)(q + r) & = & (pq + r')(r + p)(r + q) & \text{Commutatitivity (Twice)} \\ & = & (pq + r')(r + pq) & \text{Distributivity} \\ & = & (pq + r')(pq + r) & \text{Commutatitivity} \\ & = & pq & \text{Problem 6} \end{array}$$

Question 11

Boolean Algebra: Express Boolean function $E(x, y, z) = (x' + y)(xy)'(x + y' + z)$ in sum-of-products form.

$$\begin{array}{rcl} (x' + y)(xy)'(x + y' + z) & = & (x' + y)(x' + y')(x + y' + z) \\ & = & (x' + yy')(x + y' + z) \\ & = & x'(x + y' + z) \\ & = & x'x + x'y' + x'z \\ & = & x'y' + x'z \end{array}$$

Question 12

Boolean Algebra: Express Boolean function $E(x, y, z) = xy + (x + z)' + x'y'z$ in product-of-sums form.

$$
\begin{aligned}
xy + (x+z)' + x'y'z &= xy + x'z' + x'y'z \\
&= (xy + x'z' + x')(xy + x'z' + y')(xy + x'z' + z) \\
&= (xy + x')(xy + y' + x'z')(xy + x' + z) \\
&= (y + x')(x + y' + x'z')(y + x' + z) \\
&= (y + x')(y + x' + z)(x + y' + x'z') \\
&= (y + x')(x + y' + x'z') \\
&= (y + x')(x + x'z' + y') \\
&= (y + x')(x + z' + y') \\
&= (x' + y)(x + y' + z')
\end{aligned}
$$

Question 13

Prove or disprove the Boolean equation $(a'b' + c)(a + b)(b' + ac)' = a'bc$.

The equation is true.

$$
\begin{aligned}
(a'b' + c)(a + b)(b' + ac)' &= (a'b' + c)(a + b)b(a' + c') && \text{DeMorgan's Law} \\
&= (a'b' + c)b(a' + c') && \text{Absorption} \\
&= (a'b'b + cb)(a' + c') && \text{Distributivity} \\
&= (a0 + cb)(a' + c') && \text{Complement} \\
&= (0 + cb)(a' + c') && \text{Boundedness} \\
&= cb(a' + c') && \text{Identity} \\
&= a'cb + c'cb && \text{Distributivity} \\
&= a'cb + 0b && \text{Complement} \\
&= a'cb + 0 && \text{Boundedness} \\
&= a'cb && \text{Identity} \\
&= a'bc && \text{Commutativity}
\end{aligned}
$$

Question 14

Boolean Algebra: Reduce the following to an expression of a minimal number of literals (4). $abc'd + ab'c + bc'd + ab'c' + acd + a'bcd$

$$
\begin{aligned}
& abc'd + ab'c + bc'd + ab'c' + acd + a'bcd \\
&= ab'c + bc'd + ab'c' + acd + a'bcd && \text{(absorption on term 1 \& 3)} \\
&= ab'(c + c') + bc'd + acd + a'bcd && \text{(distribution on term 1 \& 3)} \\
&= ab' + bc'd + acd + a'bcd \\
&= ab' + bc'd + a(b + b')cd + a'bcd \\
&= ab' + bc'd + abcd + ab'cd + a'bcd \\
&= ab' + bc'd + abcd + a'bcd && \text{(absorption on term 1 \& 4)} \\
&= ab' + bc'd + (a + a')bcd \\
&= ab' + b(c + c')d \\
&= ab' + bd
\end{aligned}
$$