Name: ____Solutions___________ Student Number: __________________________	CISC 203 Discrete Mathematics for Computing Science Test 2 Fall 2010 Professor Mary McCollam

This test is 50 minutes long and there are 40 marks. **Please write in pen and only in the box marked "Answer".**
This is a closed-book exam. No computers or calculators are allowed.

Question 1: [10 marks]

Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$

(a) Find $A \vee B$ (Recall that $\vee$ denotes the Boolean *join* operation)

Answer:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

(b) Find $B^{[2]}$ (Recall that $B^{[2]} = B \odot B$, where $\odot$ denotes the Boolean *product* operation)

Answer:

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Question 2: [10 marks]

(a) Use the Euclidean algorithm to find gcd(3003, 357).

Answer:

3003 = (357)(8) + 147 OR gcd(3003, 357) = gcd(357, 147)
357 = (147)(2) + 63 = gcd(147, 63)
147 = (63)(2) + 21 = gcd(63, 21)
63 = (21)(3) + 0 = gcd(21, 0)

Therefore, gcd(3003, 357) = 21

(b) Convert the integer 295 from decimal notation to binary notation.

Answer:

295 / 2 = 147 rm 1
147 / 2 = 73 rm 1
73 / 2 = 36 rm 1
36 / 2 = 18 rm 0
18 / 2 = 9 rm 0
9 / 2 = 4 rm 1
4 / 2 = 2 rm 0
2 / 2 = 1 rm 0
1 / 2 = 0 rm 1

Therefore $(295)_{10} = (100100111)_2$

Question 3: [10 marks] For each of the following, show the steps leading to the solution.

(a) Find an inverse of 7 modulo 31.

Answer: Work backwards through the Euclidean algorithm to find a linear combination of 7 and 31 = gcd(7,31) = 1

$31 = (7)(4) + 3$ $\quad$ $3 = (1)(31) – (4)(7)$
$7 = (3)(2) + 1$ $\quad$ $1 = (1)(7) – (2)(3)$
$3 = (1)(3) + 0$

So, $1 = (1)(7) – (2)((1)(31) – (4)(7))$
$1 = (9)(7) – (2)(31)$

Therefore 9 is an inverse of 7 modulo 31

Also, all integers congruent to 9 modulo 31 are inverses of 7 modulo 31:

…, -53, -22 , 9, 40, 71, …

(b) Solve the congruence $7x \equiv 13 \pmod{31}$. Give the answer modulo 31.

Answer:

Multiply both sides of the congruence by an inverse of 7 modulo 31, e.g., 9

$7x \equiv 13 \pmod{31}$
$(9)(7x) \equiv (9)(13) \pmod{31}$
$63x \equiv 117 \pmod{31}$
$x \equiv 24 \pmod{31}$

Therefore, x = 24 or any integer congruent to 24 modulo 31:

… , -7, 24, 55, 86, 117, …

Question 4: [10 marks] Use *proof by contradiction* to show that the square root of 2 is irrational.

Recall that a real number x is *rational* if there exist integers *p* and *q* with $q \neq 0$ such that $x = p/q$. A real number that is not rational is called *irrational*.

HINT: Use the following facts in your proof.

- If a number is rational, it can be expressed as a fraction *p*/*q* in lowest terms, where *p* and *q* are integers, at least one of which is odd (otherwise, it wouldn't be in lowest terms, since 2 would divide both *p* and *q*).
- The square of an odd number is odd.

Answer:

Assume that the square root of 2 is rational.

Then it could be expressed as a fraction p/q in lowest terms, where p and q are integers, with at least one of those being odd.

If $p/q = \sqrt{2}$ then $p^2/q^2 = 2$

and then $p^2 = 2q^2$

Therefore p^2 must be even

Since the square of an odd number is odd, then p must also be even

If p is even, then q must be odd,

since p/q is in lowest terms, so either p or q must be odd

However, if p is even, then p^2 is a multiple of 4

If p^2 is a multiple of 4 and $p^2 = 2q^2$, then $2q^2$ is also a multiple of 4, so q is even

Therefore, we have that q is odd and q is even, which is a contradiction.

Therefore, our initial assumption, that the square root of 2 is rational, is false

Therefore, the square root of 2 is irrational.