CONCORDIA UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

COMP238 MATHEMATICS FOR COMPUTER SCIENCE I

ASSIGNMENT 3 SOLUTIONS WINTER 2009

1. If A and B are sets and $f : A \longrightarrow B$ then for any subset S of B *the pre-image of* S is

$$f^{-1}(S) \equiv \{a \in A : f(a) \in S\} \ .$$

Note that $f^{-1}(S)$ is well defined even if f does not have an inverse!

Let S and T be subsets of B. Prove that

$$f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T) \ .$$

PROOF:

$$\begin{aligned} x \in f^{-1}(S \cup T) \ &\equiv \ f(x) \in S \cup T \ \equiv \ f(x) \in S \text{ or } f(x) \in T \\ &\equiv \ x \in f^{-1}(S) \text{ or } x \in f^{-1}(T) \ \equiv \ x \in f^{-1}(S) \cup f^{-1}(T) \ . \end{aligned}$$

Prove that

$$f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T) \ .$$

PROOF:

$$\begin{aligned} x \in f^{-1}(S \cap T) \ &\equiv \ f(x) \in S \cap T \ \equiv \ f(x) \in S \text{ and } f(x) \in T \\ &\equiv \ x \in f^{-1}(S) \text{ and } x \in f^{-1}(T) \ \equiv \ x \in f^{-1}(S) \cap f^{-1}(T) \ . \end{aligned}$$

2. Show that the function $g : (\mathbf{R} - \{1\}) \longrightarrow (\mathbf{R} - \{1\})$ given by

$$g(x) = \frac{x+1}{x-1} \ ,$$

is a bijection (*i.e.*, one-to-one and onto).

SOLUTION: A function is one-to-one and onto if and only if it is invertible. Thus it suffices to show that g has an inverse. In fact $g^{-1}(x) = g(x)$, because for any $x \in \mathbf{R} - \{1\}$ we have

$$g(g(x)) \ = \ g(\frac{x+1}{x-1}) \ = \ \frac{\frac{x+1}{x-1} \ + \ 1}{\frac{x+1}{x-1} \ - \ 1} \ = \ \frac{(x+1) \ + \ (x-1)}{(x+1) \ - \ (x-1)} \ = \ x \ .$$

3. When an integer b is divided by 12, the remainder is 5. What is the remainder when $8b$ is divided by 12?

   SOLUTION: We can write $b = 12k + 5$, where k is an integer. Then $8b = 8 \cdot 12k + 40 = (8k + 3) \cdot 12 + 4$. Thus the remainder is 4.

   When an integer c is divided by 15, the remainder is 3. What is the remainder when $10c$ is divided by 15?

   SOLUTION: We can write $c = 15k + 3$, where k is an integer. Then $10c = 10 \cdot 15k + 30 = (10k + 2) \cdot 15 + 0$. Thus the remainder is 0.

4. Without computing the value of $(20!)^2$ determine how many zeros are at the end of this number when it is written in decimal form. Justify your answer.

   SOLUTION: $(20!)^2 = 20^2 \cdot 19^2 \cdot 18^2 \cdot 17^2 \cdot \cdots \cdot 3^2 \cdot 2^2$. We see that the factorization of $(20!)^2$ contains the factor 5^8, as well as the factor 2^k where $k > 8$. Thus Thus $(20!)^2$ ends with eight zeros.

5. Find all solutions to $m^2 - n^2 = 88$, for which both m and n are positive integers.

   SOLUTION: We can write this equation as $(m + n)(m - n) = 2^3 \cdot 11$. Let $p = m + n$ and $q = m - n$. We must look for integer solutions p and q of $p \cdot q = 2^3 \cdot 11$ that also satisfy $p \geq 2$, $q \geq 1$, and $p > q$. We see that the only candidate solutions that satisfy the three constraints are $(p, q) = (11 \cdot 2^0, 2^3)$, $(11 \cdot 2^1, 2^2)$, $(11 \cdot 2^2, 2^1)$, and $(11 \cdot 2^3, 2^0)$. From the equations $p = m + n$ and $q = m - n$ we find that $m = (p + q)/2$ and $n = (p - q)/2$. For the four candidate solutions this gives $(m, n) = (9.5, 1.5)$, $(13, 9)$, $(23, 21)$, $(44.5, 43.5)$. Thus there are two integer solution pairs, namely, $(m, n) = (13, 9)$, and $(m, n) = (23, 21)$.

6. Prove that if n is an odd positive integer then $n^2 \equiv 1 \pmod 8$.

   PROOF: Let n be odd, $n = 2k + 1$. ($k \geq 0$). Then $n^2 = 4k^2 + 4k + 1$. Now consider the following 2 cases (with $m \geq 0$):

   Case 1: k is even, $k = 2m$: Then $n^2 = 4(2m)^2 + 4(2m) + 1 = 8(2m^2 + m) + 1$. Thus $n^2 \bmod 8 = 1$.

   Case 2: k is odd, $k = 2m+1$: Then $n^2 = 4(2m+1)^2 + 4(2m+1) + 1 = 8(2m^2 + 2m + m) + 9 = 8(2m^2 + 2m + m + 1) + 1$. Thus $n^2 \bmod 8 = 1$.

7. Prove that for all integers n we have

$$n^3 = 9k \ , \quad \text{or} \quad n^3 = 9k+1 \ , \quad \text{or} \quad n^3 = 9k-1 \ ,$$

for some integer k.

PROOF: It suffices to consider the following three cases:

Case 1: $n = 3m$: Then $n^3 = 3^3 \cdot m^3 = 9k$, where $k = 3m^3$.

Case 2: $n = 3m+1$: Then $n^3 = (3m+1)^3 = (3m)^3 + 3 \cdot (3m)^2 + 3 \cdot (3m) + 1 = 9(3m^3 + 3m^2 + m) + 1 = 9k + 1$, where $k = 3m^3 + 3m^2 + m$.

Case 3: $n = 3m+2$: Then $n^3 = (3m+2)^3 = (3m)^3 + 3 \cdot (3m)^2 \cdot 2 + 3 \cdot (3m) \cdot 2^2 + 2^3 = 9(3m^3 + 6m^2 + 4m) + 8 = 9k - 1$, where $k = 3m^3 + 6m^2 + 4m + 1$.

8. Prove that if a, b, c, d, and m are integers, with $m \geq 2$, and

$$a \ \equiv \ b \ (\text{mod } m) \qquad \text{and} \qquad c \ \equiv \ d \ (\text{mod } m) \ ,$$

then

$$a - c \ \equiv \ b - d \ (\text{mod } m) \ .$$

PROOF: Since $a \equiv b$ (mod m) we have $a = b + k_1 m$, and since $c \equiv d$ (mod m) we have $c = d + k_2 m$, for certain integers k_1 and k_2. Thus $a - c = b - d + (k_1 - k_2)m$, *i.e.*, $a - c = b - d + km$, for some integer k ($k = k_1 - k_2$), so that $a - c \ \equiv \ b - d$ (mod m) . QED

9. Prove that if a, b, and m are integers, with $m \geq 2$, and $a \equiv b$ (mod m), then

$$\gcd(a, m) \quad = \quad \gcd(b, m) \ .$$

PROOF: Since $a \equiv b$ (mod m) we have $a = b + km$ for some integer k. Let $d = \gcd(a, m)$. Then $d|a$ and $d|m$. Since $b = a - km$ it follows that $d|b$. Thus $d|b$ and $d|m$, *i.e.*, d is a divisor of both b and m. We still must show that d is the *greatest* divisor of b and m. We do this by contradiction. Suppose that d is not the greatest divisor of b and m. There there is an integer $\hat{d}$, with $\hat{d} > d$, such that $\hat{d}|b$ and $\hat{d}|m$. Since $a = b + km$ it follows that $\hat{d}|a$. Thus $\hat{d}|a$ and $\hat{d}|m$, *i.e.*, $\hat{d}$ is a divisor of both a and m. But this contradicts that d if the greatest divisor of a and m. QED.

10. Prove the following by mathematical induction: For all integers $n \geq 1$,

$$1 + 6 + 11 + 16 + \ldots + (5n - 4) \;=\; \frac{n(5n-3)}{2} \;.$$

PROOF: If $n = 1$ then the LHS and RHS are clearly equal, with value 1. The inductive step consists of assuming that for some $n \geq 1$ we have

$$1 + 6 + 11 + 16 + \ldots + (5n - 4) \;=\; \frac{n(5n-3)}{2} \;,$$

and showing that

$$1 + 6 + 11 + 16 + \ldots + (5n - 4) + (5(n+1) - 4) \;=\; \frac{(n+1)(5(n+1)-3)}{2} \;.$$

Using the inductive assumption we have

$$\begin{aligned} 1 + 6 + 11 + 16 + \ldots + (5n - 4) + (5(n+1) - 4) \;&=\; \frac{n(5n-3)}{2} + 5(n+1) - 4 \\ = \frac{n(5n-3) + 10n + 2}{2} \;&=\; \frac{5n^2 + 7n + 2}{2} \\ = \frac{(n+1)(5n+2)}{2} \;&=\; \frac{(n+1)(5(n+1)-3)}{2}. \quad \text{QED} \end{aligned}$$

11. Prove by induction: For all integers $n \geq 1$,

$$5 \mid (7^n - 2^n) \;.$$

PROOF: If $n = 1$ then $7^n - 2^n = 7 - 2 = 5$, which is divisible by 5. The inductive step consists of assuming that for some $n \geq 1$ we have $5|(7^n - 2^n)$, and showing that $5|(7^{n+1} - 2^{n+1})$. Now $7^{n+1} - 2^{n+1} = 7 \cdot 7^n - 2 \cdot 2^n = 7(7^n - 2^n) + 5 \cdot 2^n$, of which the second term is clearly divisible by 5, while the first term is divisible by 5 by inductive assumption. QED

12. Prove by induction: For all integers $n \geq 2$,

$$n! \;>\; 2^{n-2} \;.$$

PROOF: If $n = 2$ then $n! = 2$ and $2^{n-2} = 1$, so that the inequality is satisfied. The inductive step consists of assuming that for some $n \geq 2$ we have $n! > 2^{n-2}$, and showing that $(n+1)! > 2^{n-1}$. From the inductive assumption it follows that $(n+1)! = (n+1)n! > (n+1)2^{n-2}$. Also $n + 1 > 2$ (because $n \geq 2$). Thus $(n+1)! > 2 \cdot 2^{n-2} = 2^{n-1}$. QED