LA Session Week - Number Theory

1) In general, you were told in class that for all integers a and b and positive integers n, if $a \equiv b \pmod n$, then $f(a) \equiv f(b) \pmod n$, where f is any polynomial function that operates on integers only. Using the definition of mod only, prove this specifically for the function $f(a) = a^3$.

Solution

We aim to prove the following: if $a \equiv b \pmod n$, then $a^3 \equiv b^3 \pmod n$.

If $a \equiv b \pmod n$, it follows that n | (a – b). Thus, there exists an integer c such that a – b = cn. Thus, we can rewrite a = b + cn.

$$a^3 = (b + cn)^3 = b^3 + 3b^2cn + 3b(cn)^2 + (cn)^3$$

We aim to show that $a^3 \equiv b^3 \pmod n$, which is equivalent to proving that n | (a^3 – b^3).

$$\begin{aligned} a^3 - b^3 &= b^3 + 3b^2cn + 3b(cn)^2 + (cn)^3 - b^3 \\ &= 3b^2cn + 3b(cn)^2 + (cn)^3 \\ &= n(3b^2c + 3bc^2n + c^3n^2) \end{aligned}$$

Since b, c and n are all integers, it follows that $3b^2c + 3bc^2n + c^3n^2$ is an integer. Thus, we've proven that n | (a^3 – b^3), as desired, which equivalently means that $a^3 \equiv b^3 \pmod n$.

2) Convert the following values from the bases indicated to base 10:

i) 2165_7 = 2 x 7^3 + 1 x 7^2 + 6 x 7^1 + 5 x 7^0 = 782
ii) $BCF2_{16}$ = 11 x 16^3 + 12 x 16^2 + 15 x 16^1 + 2 x 16^0 = 48370
iii) 12345_8 = 1 x 8^4 + 2 x 8^3 + 3 x 8^2 + 4 x 8^1 + 5 x 8^0 = 5349
iv) 21302_4 = 2 x 4^4 + 1 x 4^3 + 3 x 4^2 + 0 x 4^1 + 2 x 4^0 = 626
v) 101001111101_2 = 2^{11} + 2^9 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^0 = 2685

3) Convert the following base 10 values to the bases indicated:

i) 22111 to base 12
12 | 22111
12 | 1842 r 7
12 | 153 r 6
12 | 12 r 9
12 | 1 r 0
$22111_{10} = 10967_{12}$

ii) 83810 to base 16

16 | 83810
16 | 5238 r 2
16 | 327 r 6
16 | 20 r 7
16 | 1 r 4
$83810_{10} = 14762_{16}$

iii) 907 to base 2

2 | 907
2 | 453 r 1
2 | 226 r 1
2 | 113 r 0
2 | 56 r 1
2 | 28 r 0
2 | 14 r 0
2 | 7 r 0
2 | 3 r 1
2 | 1 r 1
$907_{10} = 1110001011_2$

iv) 3209 to base 7

7 | 3209
7 | 458 r 3
7 | 65 r 3
7 | 9 r 2
7 | 1 r 2
$3209_{10} = 12233_7$

v) 4095 to base 8

8 | 4095
8 | 511 r 7
8 | 63 r 7
8 | 7 r 7
$4095_{10} = 7777_8$

4) Prove or disprove: if n is an integer, then n(3n+1) is an even integer.

There are two cases: (a) n is even, (b) n is odd.

In case (a), there exists an integer c such that n = 2c.

n(3n+1) = (2c)(3n+1) = 2(c(3n+1)), since c and n are integers, c(3n+1) is an integer, thus, in this case, we can conclude that n(3n+1) is even.

In case (b), there exists an integer c such that n = 2c + 1.

n(3n+1) = n (3(2c+1)+1) = n(6c+3+1) = n(6c + 4) = 2n(3c + 2), since n and c are integers, it follows that n(3c+2) is an integer. Thus, we can conclude, in this case, that n(3n+1) is even.

Since in both possible cases n(3n+1) is even, we can conclude that this expression is even for all integers n.

5) Prove or disprove: if n(3n+1) is an even integer, then n is an integer.

This claim is false! Consider plugging in n = $\frac{2}{3}$ into the expression:

$$n(3n+1) = \frac{2}{3}\left(3\left(\frac{2}{3}\right)+1\right) = \frac{2}{3}(2+1) = 2$$

Thus, in this situation, we have that n(3n+1) is even (equal to 2), but the corresponding value of n, which is 2/3, is NOT an integer.

Note: This counter example was reached by setting n(3n+1) equal to 2, and then solving the ensuing quadratic equation which had one integral and one non-integral root. The latter was used for the counter example.