COT 3100 Fall 2017 Homework #3 Solutions

1) In general, you were told in class that for all integers a and b and positive integers n, if $a \equiv b \ (mod\ n)$, then $f(a) \equiv f(b) \ (mod\ n)$, where f is any function that operates on integers only. Using the definition of mod only, prove this specifically for the function $f(a) = a^2$.

Solution
We must show that if $a \equiv b \ (mod\ n)$, then $a^2 \equiv b^2 \ (mod\ n)$.

We must prove that n | (a^2 - b^2) by definition of mod.
Note that if $a \equiv b \ (mod\ n)$, then n | (a-b).
Thus, there exists an integer c such that a - b = nc.

$a^2 - b^2 = (a - b)(a + b) = nc(a + b)$

Since a, b, and c are integers, we've proven that $a^2 - b^2$ is divisible by n. It follows that the original assertion is true.

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

Solution
i) $3645_7 = 3 \times 7^3 + 6 \times 7^2 + 4 \times 7^1 + 5 \times 7^0 = 1029 + 294 + 28 + 5 = 1356$

ii) $AAF7_{16} = 10 \times 16^3 + 10 \times 16^2 + 15 \times 16^1 + 7 = 4096 + 2460 + 240 + 7 = 42767$

iii) $12345_9 = 1 \times 9^4 + 2 \times 9^3 + 3 \times 9^2 + 4 \times 9^1 + 5 = 6561 + 1458 + 243 + 36 + 5 = 8303$

iv) $30020_4 = 3 \times 4^4 + 2 \times 4^1 = 768 + 8 = 776$

v) $101101011001_2 = 2^{11} + 2^9 + 2^8 + 2^6 + 2^4 + 2^3 + 2^0 = 2048 + 512 + 256 + 64 + 16 + 8 + 1 = 2905$

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

Solution

i) 12435 to base 12

12 | 12435
12 | 1036 R 3
12 | 86 R 4
12 | 7 R 2
12 | 0 R 7
The converted value is 7243_{12}.

ii) 79770 to base 16

16 | 79770
16 | 4985 R 10 (A)
16 | 311 R 9
16 | 19 R 7
16 | 1 R 3
16 | 0 R 1
The converted value is $1379A_{16}$.

iii) 691 to base 2

2 | 691
2 | 345 R 1
2 | 172 R 1
2 | 86 R 0
2 | 43 R 0
2 | 21 R 1
2 | 10 R 1
2 | 5 R 0
2 | 2 R 1
2 | 1 R 0
2 | 0 R 1
The converted value is 1010110011_2.

iv) 4921 to base 7

7 | 4921
7 | 703 R 0
7 | 100 R 3
7 | 14 R 2
7 | 2 R 0
7 | 0 R 2
The converted value is 20230_7.

v) 88264 to base 8

8 | 88264
8 | 11033 R 0
8 | 1379 R 1
8 | 172 R 3
8 | 21 R 4
8 | 2 R 5
8 | 0 R 2
The converted value is 254310_8.

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

Solution
We consider two cases: 1) when n is even and 2) when n is odd. The proof for both cases follows:

Case 1: n is even. There exists an integer c such that n = 2c. Then we have

n(3n+1) = 2c(3(2c) + 1) = 2c(6c+1), since c is an integer, it follows that this quantity is even, since we've expressed it as 2 times an integer.

Case 2: n is odd. There exists an integer c such that n = 2c + 1. Then we have

n(3n+1) = (2c + 1)(3(2c + 1) + 1) = (2c + 1)(6c + 3 + 1) = (2c+1)(6c +4) = 2(2c+1)(3c+2)

Since c is an integer, it follows that the quantity is even, since we've expressed it as 2 times an integer.

5) Prove that if n is an odd integer, then $n^4 \equiv 1\ (mod\ 16)$. You may use the result from problem 4 to aid you in this proof. (Hint: At some point when you do your algebra, you should get an expression of the form a(3a + 1) where a is an integer. It is extremely helpful when you get to this point to use the result proved in question 4.)

Solution
Since n is odd, there exists an integer c such that n = 2c + 1. Now, we proceed as follows:

$$\begin{aligned} n^4 &= (2c+1)^4 \\ &= 16c^4 + 32c^3 + 24c^2 + 8c + 1 \\ &= 16(c^4 + 2c^3) + 8c(3c+1) + 1 \end{aligned}$$

Using the result above, there exists an integer d such tnat $c(3c+1) = 2d$. We substitute accordingly:

$$\begin{aligned} &= 16(c^4 + 2c^3) + 8(2d) + 1 \\ &= 16(c^4 + 2c^3) + 16d + 1 \\ &= 16(c^4 + 2c^3 + d) + 1 \\ &\equiv 1\ (mod\ 16) \end{aligned}$$

Since c and d are integers, the whole expression on the second to left line that is expressed as a product of 16 and an integer drops out when considering it mod 16.

6) Let x and y be integers such that 12 | (3x + 4y). Prove that 12 | (21x + 16y).

Solution

Note that the given information infers that there exists an integer a such that

$$3x + 4y = 12\,a.$$

We start with the given quantity and aim to rewrite it as 12 times an integer:

$$\begin{aligned} 21x + 16y &= (36x - 15x) + (36y - 20y) \\ &= 36(x + y) - 5(3x + 4y) \\ &= 12(3x + 3y) - 5(12a) \\ &= 12(3x + 3y - 5a) \end{aligned}$$

Since x, y and a are all integers, we've expressed the original quantity as 12 times an integer, proving that it is divisible by 12, as desired.

7) Give a summary of the life and mathematical contributions of Evariste Galois. Please aim for a length of roughly 200 - 400 words. ***Your summary must be typed.*** Please state the sources you used in writing your summary.

Sample Write Up

Galois was a 19th century French mathematician who essentially started the mathematical field of Group Theory. At a very young age he showed an extreme affinity for mathematics in school. By the time he was 15, he was already reading papers by Lagrange. He always wanted to attend the Ecole Polytechnique, one of the top schools in France, but ultimately had to settle on going to the Ecole Normale. At the age of 18, he graduated from the Ecole Normale, where he had attempted to publish his paper on equation theory. Although this work turned out to be extremely important, it was never published in his short life time and was only posthumously discovered. While still 18, Galois published three papers that would lay the groundwork for Galois theory and finite fields. Much of the current mathematical background necessary to create public key cryptosystems is based on groups and finite fields. Unfortunately, Galois's political life was quite turbulent. In between the ages of 18 and 20, he was imprisoned multiple times for his political activity, as he was seen to be against the current king, Louis Philippe. Unfortunately, he didn't get a chance to truly expound upon the field of mathematics he created because he died in a duel over a woman (at least the evidence supports this) in 1832 at the age of 20.
(Source: Wikipedia, https://en.wikipedia.org/wiki/%C3%89variste_Galois)