ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 18

Solutions to Homework 9

Introduction to Communication Systems December 26, 2009

PROBLEM 1. 1. Since $a \equiv a'$; (mod m), it implies that a - a' = km for some integer k. On the other hand we have:

$$a^{t} - a^{\prime t} = (a - a^{\prime})(a^{t-1} + a^{t-2}a^{\prime} + \dots + a^{\prime t-1}) = mk(a^{t-1} + a^{t-2}a^{\prime} + \dots + a^{\prime t-1})$$

Therefore, $a^t - a'^t$ is divisible by m, which implies that $a^t \equiv a'^t$; (mod m).

2. The converse is not necessarily true. For example $(-1)^2 \equiv (+1)^2$; (mod 5) but $(-1) \neq (+1) \pmod{5}$.

PROBLEM 2. We have

 $a^{3} + 3 = a^{3} + 27 - 24 = a^{3} + 3^{3} - 24 = (a+3)(a^{2} - 3a + 9) - 24$

So, if $a^3 + 3$ is devisible by a + 3, $(a + 3)(a^2 - 3a + 9) - 24$ should be also divisible by a + 3. Therefore 24 is devisible by a + 3. But we know that the only factors of 24 are : 1, 2, 3, 4, 6, 8, 12, 24. This means that a + 3 should be one of these numbers. Since a is assumed to be a positive integer number, the only possibilities for a are a = 1, 3, 5, 9, or 21.

PROBLEM 3. Since n is assumed to be an odd number, we can write n = 2k + 1

1. We have:

$$n^{2} - 1 = (n - 1)(n + 1) = (2k + 1 - 1)(2k + 1 + 1) = (2k)(2k + 2) = 4k(k + 1).$$

Notice that k and k + 1 are two consecutive numbers. Therefore one of them is even and the other one is odd. In both cases, the product of them is an even number. So, k(k+1) = 2m. Therefore:

$$n^{2} - 1 = 4k(k+1) = 4(2m) = 8m.$$

This shows that $n^2 - 1$ is a multiple of 8.

2. We will factor $n^8 - 1$ as:

$$n^{8} - 1 = (n^{4} - 1)(n^{4} + 1) = (n^{2} - 1)(n^{2} + 1)(n^{4} + 1).$$

From the first part of the question we know that $n^2 - 1$ is divisible by 8. So, $n^2 - 1 = 8m$. Also, we know that the other factors are even numbers, since n is an odd number. Therefore we have:

$$n^{8} - 1 = (n^{2} - 1)(n^{2} + 1)(n^{4} + 1) = 8m \times 2l \times 2p = 32mlp.$$

This shows that $n^8 - 1$ is divisible by 32.

PROBLEM 4. First we write the congruence equation as

$$7n \equiv -5$$
; (mod 2009)

Now, we need to find $7^{-1} \pmod{2009}$. Using Euclid's algorithm, we can show that $7^{-1} \equiv 287$; (mod 2009). Now, if we multiply both sides of the equation with 287 we have:

$$287 \times 7n \equiv 287 \times (-5); (\mod 2009)$$

Therefore :

$$n \equiv -1435 \equiv 574; (\mod 2009).$$