ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

**Handout 17** | Introduction to Communication Systems
Solutions to Homework 9 | November 13, 2008

Problem 1. 1. We see that

$$4^2 = 16 \equiv 1 \pmod{15}$$

Thus by exponentiating the above congruence we get

$$(4^2)^4 \equiv 1 \pmod{15}$$

2. We have that $180 = 3 \times 5 \times 3 \times 4$. First notice that

$$26 \equiv -3 \pmod{29}$$

Thus

$$(26)^3 \equiv (-3)^3 \equiv -27 \equiv 2 \pmod{29}$$

Now taking the fifth power we get

$$((26)^3)^5 \equiv 2^5 \equiv 32 \equiv 3 \pmod{29}$$

Taking the third power we get

$$(((26)^3)^5)^3 \equiv 3^3 \equiv 27 \equiv -2 \pmod{29}$$

Finally taking the fourth power we get

$$26^{180} = ((((26)^3)^5)^3)^4 \equiv (-2)^4 \equiv 16 \pmod{29}$$

Thus

$$26^{180} \equiv 16 \pmod{29}$$

3. The last two digits of any number belongs to the set $\{00, 01, 02, 03, 04 \ldots, 97, 98, 99\}$. This set can be easily identified as the set of numbers modulo 100. Thus to find the last two digits $7^{20}$ we must find its modulo w.r.t 100. We have

$$7^4 = 2401 \equiv 1 \pmod{100}$$

Thus

$$7^{20} = (7^4)^5 \equiv 1 \pmod{100}$$

Thus the last two digits of $7^{20}$ are $0, 1$.

Problem 2. We know from the Bezout's theorem that for any integers $a, b$

$$\gcd(a, b) = \alpha a + \beta b$$

for some integers $\alpha, \beta$. Note that if the $\gcd(a, b) = 1$, then we have that

$$\alpha a = -\beta b + 1$$

Thus

$$\alpha a \equiv 1 \pmod{b}$$

As a result we have that $\alpha = (a)^{-1} \pmod{b}$.

1. Using the extended Euclid's algorithm we have

$$\gcd(7, 26) = 1 = (-11)7 + (3)26$$

Thus $-11 \equiv 15 \equiv (7)^{-1} \pmod{26}$.

2. Using the extended Euclid's algorithm we have

$$\gcd(13, 37) = 1 = (-17)13 + (6)37$$

Thus $-17 \equiv 20 \equiv (13)^{-1} \pmod{37}$.

Problem 3.
1. Since $m$ is a prime number the only integers in $1, 2, \ldots, m^3$ which have a factor common with $m$ are the multiples of $m$. The multiples of $m$ less than $m^3$ are $\{1 \cdot m, 2 \cdot m, 3 \cdot m, \ldots, m^2 \cdot m\}$. Thus there are $m^2$ multiples of $m$. As a result

$$\phi(m^3) = m^3 - m^2 = m^2(m-1).$$

2. In general we again apply the same trick and count the number of integers less than $m^n$ which are multiples of $m$, since they are the only numbers with a factor common to $m$. These are $\{1 \cdot m, 2 \cdot m, 3 \cdot m, \ldots, m^2 \cdot m, \ldots, m^{n-1} \cdot m\}$. There are $m^{n-1}$ such numbers, thus

$$\phi(m^n) = m^n - m^{n-1} = m^{n-1}(m-1).$$

Problem 4.
1. $30 = 2 \times 3 \times 5$. We know that if $m, n$ are relatively prime then $\phi(mn) = \phi(m)\phi(n)$. Thus $\phi(30) = \phi(2)\phi(3)\phi(5)$. And for any prime number $m$, $\phi(m) = m - 1$. Thus $\phi(30) = (2-1)(3-1)(5-1) = 8$.

2. We know from the Euler's theorem that if $a, m$ are relatively prime then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

This implies that

$$a^{\phi(m)-1} a \equiv 1 \pmod{m}.$$

Thus $a^{\phi(m)-1} \equiv a^{-1} \pmod{m}$. In this problem since $13, 30$ are relatively prime (since 13 is a prime number), we have

$$13^{\phi(30)-1} = 13^7 \equiv \pmod{30}$$

using the fact that $\phi(30) = 8$. But

$$\begin{aligned}
13^2 &= 169 \equiv -11 \pmod{30} \\
13^4 &\equiv (-11)^2 \equiv 121 \equiv 1 \pmod{30} \\
13^6 &= (13^4)(13^2) \equiv (-11)(1) \pmod{30} \\
13^7 &= (13^6)(13) \equiv (-11)(13) \equiv 7 \pmod{30}
\end{aligned}$$

Thus $7 \equiv 13^{-1} \pmod{30}$.

Problem 5.

1. We enumerate $x$ starting from 0 to see that $x = 7$ satisfes the congruence equation.
2. This congruence equation does not have a solution for $x$. To prove this let us assume that there exists a number $x \geq 0$ such that $2^x \equiv 3 \pmod{12}$. This implies that 12 divides $2^x - 3$. This is not possible since $2^x - 3$ is an odd number and 12 is an even number.