MATH 240: Discrete Structures 1 Assignment #2

Monorina Mukhopadhyay (ID: 260364335)

October 22, 2017

Problem 1

$$N \equiv 2mod3 \qquad (1)$$
$$N \equiv 1mod5 \qquad (2)$$
$$N \equiv 4mod7 \qquad (3)$$

First, I use the Chinese Remainder Theorem to solve (1) and (2). 1 can be written as

$$1 = 3m_1 + 5m_2$$

[b = 5, a = 3]   5 = 3x1 + 2
[b = 3, a = 2]   3 = 2x1 + 1
1 = 3 - 2 = 3 - (5 - 3) = 2 · 3 - 5
From the Chinese Remainder Theorem, $x = 3m_1a_2 + 5m_2a_1 = 3 \cdot 2 \cdot 1 - 5 \cdot 2 = -4$ solves (1) and (2)
Since -4 is less than n_1n_2, and x mod y ≡ x if x < y, $-4 \equiv -4mod15 \equiv 11mod15$
Now, the two equations to solve are:

$$N \equiv 11mod15$$
$$N \equiv 4mod7$$

Using the Chinese Remainder Theorem again: [b = 15, a = 7]   15 = 7 · 2 + 1
1 = 15 - 7 · 2
N = 4(15) - 7(11)(2) = -94 ≡ -94 mod 105 ≡ 11 mod 105 = 11
Check:
11 mod 3 ≡ 2 mod 3
11 mod 5 ≡ 1 mod 5
11 mod 7 ≡ 4 mod 7

Problem 2

a Need to find x,y such that 60 | xy, 60 ∤ x and 60 ∤ y
By inspection, for any x < 60 and y < 60, such that xy = 60k (where k is an integer), this will work.
For example, for x = 15, y =4: 15 mod 60 ≢ 0 mod 60 and 4 mod 60 ≢ 0 mod 60 but 15 · 4 mod 60 ≡ 0 mod 60.
The same also holds true for x = 12, y =10, where xy mod 60 ≡ 0 mod 60, but x mod 60 ≢ 0 mod 60 and y mod 60 ≢ 0 mod 60

b x, y integers, p prime and xy mod p ≡ 0 $\implies$ xy = pt
Assume p does not divide x $\implies$ gcd(p,x) = 1 $\implies$ 1 = m_1p + m_2 x
$\implies$ y = $m_1$py + $m_2$xy $\implies$ y = $m_1$py + $m_2$pt = p(m_1y + m_2t) $\implies$ p | y.
Since x was picked randomly, the same holds true if x and y are reversed. Therefore, if a prime number divides the product of two integers, it must divide at least one of the two integers.

Problem 3

Given: m | N and n | N $\implies$ N = mt_1 and N = nt_2
Since m and n are relatively prime, gcd(m,n) = 1 $\implies$ N = $a_1mN + a_2nN = a_1mnt_2 + a_2nmt_1 = (a_1t_2 + a_2t_1)mn$ $\implies$ mn | N

Problem 4

a > 2 and n $\geq$ 1, a, n $\in \mathbb{Z}$
Need to prove that: $a-1|a^n-1$
Proof by induction:
Base case: $a>2, n=1; a^n-1=a-1 \implies (a-1)|(a-1)$ so base case holds
Induction hypothesis: Assume $a-1|a^k-1 \implies a^k-1=(a-1)t$ for an integer t
Induction Step: For k+1, $a^{k+1}-1=a^{k+1}-a^k+a^k-1=a^k(a-1)+(a^k-1)=a^k(a-1)+(a-1)t=(a-1)(a^k+t) \implies a-1|a^{k+1}-1$

Problem 5

$x \in 0,1,2....,38$ For x to satisfy $x^{39}-x \equiv 0$ mod 39 means that 39 | $x^{39}-x$.
Since 39 = 13 $\cdot$ 3, and gcd(13,3) = 1, this means that 13 | $x^{39}-x$ and 3| $x^{39}-x$
This is easily proved as below:
Let $x^{39}-x=N$. 39 |N $\implies$ N = 39k = 13$\cdot$3k = 13 (3k) and N=3(13k) $\implies$ 13 | N and 3 | N Solving these two equations using the Chinese Remainder Theorem:
13 = 3(4) + 1 $\implies$ 1 = 13 - 3(4) $\implies$ x = $x^{39} \cdot 13 - 3 \cdot 4 \cdot x^{39} = x^{39}$ $x = x^{39}$ is only true for x= 0 or x = 1. For any higher x, x^{39} is always > x. So there are only two values of x for which the equation holds true.

Problem 6

Using the dynamic programming algorithm for fast algorithm shown in class: $22^{362}=(22^{181})$
$=(22^2)(22^{180})^2$
$=22^2(22^{90})^4$
$=22^2(22^{45})^8$
$=22^2 22^8(22^{44})^8$
$=22^2 22^8(22^{22})^{16}$
$=22^2 22^8(22^{11})^{32}$
$=22^2 22^8(22^{32})(22^{10})^{32}$
$=22^2 22^8 22^{32}(22^5)^{64}$
$=22^2 22^8 22^{32} 22^{64}(22^4)^{64}$
$=22^2 22^8 22^{32} 22^{64}(22^2)^{128}$
$=22^2 22^8 22^{32} 22^{64}(22)^{256}$ 22^{362} mod 12 = $22^2 22^8 22^{32} 22^{64}(22)^{256}$ mod 12.
22^1 mod 12 = 10 mod 12 = 10.
22^2 mod 12 = $(22^1 \cdot 22^1)$ mod 12
= (22 mod 12) (22 mod 12) mod 12 $\equiv 10 \cdot 10$ mod 12 $\equiv 4 mod 12$
22^4 mod 12 = $(22^2 mod 12)(22^2 mod 12) mod 12$
$\equiv 16 mod 12 \equiv 4 mod 12$
$22^8 mod 12 = (22^4 mod 12)(22^4 mod 12) mod 12 \equiv 16 mod 12 \equiv 4 mod 12$
$\implies$, all higher powers of 22 will also reduce to 4 mod 12 since they can always be expressed as (4 mod 12)(4 mod 12) mod 12.
$22^{362} mod 12 = 22^2 22^8 22^{32} 22^{64}(22)^{256}$ mod 12 $\equiv (4 \cdot 4 \cdot 4 \cdot 4 \cdot 4) mod 12 \equiv 4^5 mod 12 \equiv 4 \cdot 4^2 \cdot 4^2 mod 12 \equiv 4 \cdot 4 \cdot 4 mod 12 \equiv$ (4 mod 12)(4 mod 12) $\equiv$ 4 mod 12.