# CS3626 Homework 01 Spring 2024

# Numeric Theory

**Total Points: 25**

Be as brief as possible and use your own words when describing concepts.   SHOW ALL WORK for Questions requiring calculations and algorithms.

Q-1: Calculate the following modular arithmetic values in the table below. (Completed example in row 1)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Expression | Dividend(a) | Quotient(q) | Modulus(b) | Remainder(r) | (b | a) true? |
| i | 39mod45 | 39 | 0 | 45 | 39 | FALSE |
| ii | 123mod-23 | -123 | -6 | 23 | 15 | FALSE |
| iii | 232517mod1027 | 232517 | 226 | 1027 | 415 | FALSE |
| iv | -147mod21 | -147 | -7 | 21 | 0 | TRUE |
| v | 0modN | 0 | 0 | N | 0 | TRUE |
| vi | N mod 0 | N | N | 0 | N | FALSE |

**N can be any positive integer > 0.**

(i) calculations:

**EXAMPLES:**

**39 mod 45 a = 39, b = 45 39 = q\*45 + r q = 0, r = 39 satisfies**

**139 mod 45 a = 139, b = 45 139 = q\*45+r q = 3 then 139 = 3\*45 + r | 0 <= r < 45 ∴ 139 – 3\*45 = r = 4**

* Or you can do long divisions to find q and r.

(ii) calculations

**123mod-23 🡺 -123 mod 23 🡺 -123 = 23(-6) + 15 🡺 0 <= r < b 🡺 0 <= 15 < 23**

(iii) calculations

**232,517mod1,027 🡺 232,517 = q(1027) + r 🡺 232,517 = 226(1027) + 415**

(iv) calculations

**-147mod21 🡺 -147 = q(21) + r, q = -7, r = 0 🡺 -147 = -7(21) + 0**

(v) and (vi)

0modN 🡺 0 = q(N) + r 🡺 0 = 0(N) + 0

N mod 0 🡺 N = q(0) + r 🡺 N = N(0) + N

**4 points**

Q-2: Using the Euclidian Algorithm, find the GCD of the following pairs, SHOW ALL WORK steps/logic.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Expression | GCD | Is Relatively Prime? |
| i | GCD(41,121) | 1 | Yes |
| ii | GCD(133,-21) | 7 | No |
| iii | GCD(1735,22) | 1 | yes |

(i)

GCD(41, 121), a > b false so swap 🡺 GCD(121, 41)

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | q | r |
| 121 | 41 | 2 | 39 |
| 41 | 39 | 1 | 2 |
| 39 | 2 | 19 | 1 |
| 2 | 1 | 2 | 0 |

(ii)

GCD(133, -21) = GCD(133, 21) = 7

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | q | r |
| 133 | 21 | 6 | 7 |
| 21 | 7 | 3 | 0 |

(iii)

GCD(1735, 22) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | q | r |
| 1735 | 22 | 78 | 19 |
| 22 | 19 | 1 | 3 |
| 19 | 3 | 6 | 1 |
| 3 | 1 | 3 | 0 |

**3 points**

Q-3: Show all work for each step of the calculation:

1. Given the equation ***y = gx mod p*** calculate y for (g,x,p) equal to:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Y** | **G** | **X** | **P** |
| i | -4 | 17 | -1 | 23 |
| ii | 11 | 2 | 140251 | 13 |
| iii | 13 | 30 | 325 | -17 |
| iv | 2 | -17 | 20 | 7 |

(i) Calculations

Y = 17^-1 mod 23

(17\*x)mod23 = 1, x will be the inverse of 17

Algorithm:

First: Start with the Euclidean algorithm

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | b | q | r | t1 | t2 | t |
| 23 | 17 | 1 | 6 | 0 | 1 | -1 |
| 17 | 6 | 2 | 5 | 1 | -1 | 3 |
| 6 | 5 | 1 | 1 | -1 | 3 | -4 |
| 5 | 1 | 5 | 0 | 3 | -4 | 23 |
| 1 | 0 | X | X | -4 | 23 | X |

17x = 1 mod 23

1 = 17(-4) mod 23 🡺 1 = -68 mod 23

(ii) Calculations

Y = 2^140251 mod 13

2^1 mod 13 = 2

2^2 mod 13 = 4

2^4 mod 13 = 3

2^8 mod 13 = 9

2^16 mod 13 = 3

2^32 mod 13 = 9

2^64 mod 13 = 3

2^128 mod 13 = 9

2^256 mod 13 = 3

2^512 mod 13 = 9

2^1024 mod 13 = 3

2^2048 mod 13 = 9

2^4096 mod 13 = 3

2^8192 mod 13 = 9

2^16384 mod 13 = 3

2^32768 mod 13 = 9

2^65536 mod 13 = 3

2^131072 mod 13 = 9

2^140251 mod 13 = (2^131072 \* 2^8192 \* 2^512 \* 2^256 \* 2^128 \* 2^64 \* 2^16 \* 2^8 \* 2^2 \* 2^1) mod 13

…………………. = (9 \* 9 \* 9 \* 3 \* 9 \* 3 \* 3 \* 9 \* 4 \* 2) mod 13

…………………. = 12,754,584 mod 13 = 11

(iii) Calculations

Y = 30^325 mod -17

swap

Y = (-30)^325 mod 17

-30^1 mod 17 = 4

-30^2 mod 17 = 1

-30^4 mod 17 = 16

-30^8 mod 17 = 16

-30^16 mod 17 = 16

-30^32 mod 17 = 16

-30^64 mod 17 = 16

-30^128 mod 17 = 16

-30^256 mod 17 = 16

-30^325 mod 17 = (-30^256) \* (-30^64) \* (-30^4) \* (-30^1) mod 17

……………….. = 16 \* 16 \* 16 \* 4 mod 17

………………. = 13

(iv) Calculations

**Y = -17^20 mod 7**

**-17^1 mod 7 = 4**

**-17^2 mod 7 = 5**

**-17^4 mod 7 = 3**

**-17^8 mod 7 = 5**

**-17^16 mod 7 = 3**

**-17^16 mod 7 🡺 (-17^16) \* (-17^4) mod 7 🡺 3 \* 3 mod 7 = 2**

**9 points**

Q-4: Using the Extended Euclidean calculate for the following:

SHOW ALL WORK calculations/steps/graphs used to complete the answer.

Find the values of d, x and y:

1. d = GCD(a = 1735, b = 22) and the (x, y) where d = ax + by = gcd(a,b)

s= s1 – s2 \* q

t = t1 – t2 \* q

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | a | b | q | r | S1 | S2 | S | t1 | t2 | t |
| 0 | 1735 | 22 | 78 | 19 | 1 | 0 | 1-0\*78 = 1 | 0 | 1 | 0-1(78) = -78 |
| 1 | 22 | 19 | 1 | 3 | 0 | 1 | 0-1(1)=-1 | 1 | -78 | 1--78(1) = 157 |
| 2 | 19 | 3 | 6 | 1 | 1 | -1 | 1--1\*6 = 7 | -78 | 79 | -78-79(6) = -552 |
| 3 | 3 | 1 | 3 | 0 | -1 | 7 | X | 79 | -552 | X |

GCD(1735, 22) = 1

1 = 1735(7) + 22(-552)

Are numeric pairs Relatively Prime? Yes

1. d = GCD(a = -357, b = -1809) 🡺 GCD(1809, 357) and the (x,y) where d = ax + by = gcd(a,b)

s= s1 – s2 \* q

t = t1 – t2 \* q

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | a | b | q | r | S1 | S2 | S | T1 | T2 | T |
| 0 | 1809 | 357 | 5 | 24 | 1 | 0 | 1 | 0 | 1 | -5 |
| 1 | 357 | 24 | 14 | 21 | 0 | 1 | -14 | 1 | -5 | 71 |
| 2 | 24 | 21 | 1 | 3 | 1 | -14 | 15 | -5 | 71 | -76 |
| 3 | 21 | 3 | 7 | 0 | -14 | 15 | x | 71 | -76 | x |

GCD(1809, 357) = 3, 1809(15) + 357(-76) = 3

Are the numeric pairs Relatively Prime? No

1. d = GCD(a = 127, b = -101) 🡺 GCD(127, 101) and the (x,y) where d = ax + by = gcd(a,b)

s = s1-s2(q)

t = t1-t2(q)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | a | b | q | r | S1 | S2 | S | t1 | t2 | t |
| 0 | 127 | 101 | 1 | 26 | 1 | 0 | 1 | 0 | 1 | -1 |
| 1 | 101 | 26 | 3 | 23 | 0 | 1 | -3 | 1 | -1 | 4 |
| 2 | 26 | 23 | 1 | 3 | 1 | -3 | 4 | -1 | 4 | -5 |
| 3 | 23 | 3 | 7 | 2 | -3 | 4 | -31 | 4 | -5 | 39 |
| 4 | 3 | 2 | 1 | 1 | 4 | -31 | 35 | -5 | 39 | -44 |
| 5 | 2 | 1 | 2 | 0 | -31 | 35 | X | 39 | -44 | 127 |

GCD(127, 101) = 1

1 = 127(35) + 101(-44)

Are numeric pairs Relatively Prime? Yes

**9 points**

**Submission Guidelines:**

* No handwritten submission is accepted, always submit answers as text within this or similar document file with any support images embedded in the file.
* **EXCEPTION**: If asked for source code implementation you can submit those individually and as separate files in ASCII format in their original file format .cpp, .java, .py, .cs etc. or even as a .txt file will be acceptable. Do not insert code into the submission document file. It ruins spacing which makes .python and some languages (perl, awk etc.) difficult to test build.
* Do not submit ZIP files… ever… for anything in D2L. The system is extremely unhelpful with regards to those filetypes and grading.
* You may include your freehand drawing/image and handwritten scans in the submission. However, the writing and images must be clearly legible. Though, it is best to present non-handwritten submissions, generally, as is done in the professional setting.
* If asked, show all work/calculations/graphs etc. in the determination of the problem.
* **Please complete your entire work in a single Word Document and Save the file as: yournetid\_CS3502\_Assignment01.docx (e.g. ogarcia5\_CS3502\_Assignment01.docx.) and upload your file in D2L.**
* Please observe the submission due date and time. After the due date there is a 50% penalty for the next 24 hours. Any submission after 24 hours of the due date will be graded at 0%.
* If you include a reference or an image taken from other sources, please cite them appropriately. APA is preferred but cite them so they can be found. **NOTE: verbatim copying or even paraphrasing is plagiarism so if the source used constitutes your answer rather than simply *supporting* the answer, it will be considered invalid. This is especially true of source code implementation answers.**
* If you resubmit, please make sure to attach the file again. Your latest submission before the due date will be the one graded.