INF638 Homework1

Jun Rao

jr2339@nau.edu

Primer Number A = 17

Multiplication table for A =17

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 |
| 3 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 27 | 30 | 33 | 36 | 39 | 42 | 45 | 48 |
| 4 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 |
| 5 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 | 55 | 60 | 65 | 70 | 75 | 80 |
| 6 | 6 | 12 | 18 | 24 | 30 | 36 | 42 | 48 | 54 | 60 | 66 | 72 | 78 | 84 | 90 | 96 |
| 7 | 7 | 14 | 21 | 28 | 35 | 42 | 49 | 56 | 63 | 70 | 77 | 84 | 91 | 98 | 105 | 112 |
| 8 | 8 | 16 | 24 | 32 | 40 | 48 | 56 | 64 | 72 | 80 | 88 | 96 | 104 | 112 | 120 | 128 |
| 9 | 9 | 18 | 27 | 36 | 45 | 54 | 63 | 72 | 81 | 90 | 99 | 108 | 117 | 126 | 135 | 144 |
| 10 | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 | 110 | 120 | 130 | 140 | 150 | 160 |
| 11 | 11 | 22 | 33 | 44 | 55 | 66 | 77 | 88 | 99 | 110 | 121 | 132 | 143 | 154 | 165 | 176 |
| 12 | 12 | 24 | 36 | 48 | 60 | 72 | 84 | 96 | 108 | 120 | 132 | 144 | 156 | 168 | 180 | 192 |
| 13 | 13 | 26 | 39 | 52 | 65 | 78 | 91 | 104 | 117 | 130 | 143 | 156 | 169 | 182 | 195 | 208 |
| 14 | 14 | 28 | 42 | 56 | 70 | 84 | 98 | 112 | 126 | 140 | 154 | 168 | 182 | 196 | 210 | 224 |
| 15 | 15 | 30 | 45 | 60 | 75 | 90 | 105 | 120 | 135 | 150 | 165 | 180 | 195 | 210 | 225 | 240 |
| 16 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240 | 256 |

Multiply modulo 17

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
| 3 | 3 | 6 | 9 | 12 | 15 | 1 | 4 | 7 | 10 | 13 | 16 | 2 | 5 | 8 | 11 | 14 |
| 4 | 4 | 8 | 12 | 16 | 3 | 7 | 11 | 15 | 2 | 6 | 10 | 14 | 1 | 5 | 9 | 13 |
| 5 | 5 | 10 | 15 | 3 | 8 | 13 | 1 | 6 | 11 | 16 | 4 | 9 | 14 | 2 | 7 | 12 |
| 6 | 6 | 12 | 1 | 7 | 13 | 2 | 8 | 14 | 3 | 9 | 15 | 4 | 10 | 16 | 5 | 11 |
| 7 | 7 | 14 | 4 | 11 | 1 | 8 | 15 | 5 | 12 | 2 | 9 | 16 | 6 | 13 | 3 | 10 |
| 8 | 8 | 16 | 7 | 15 | 6 | 14 | 5 | 13 | 4 | 12 | 3 | 11 | 2 | 10 | 1 | 9 |
| 9 | 9 | 1 | 10 | 2 | 11 | 3 | 12 | 4 | 13 | 5 | 14 | 6 | 15 | 7 | 16 | 8 |
| 10 | 10 | 3 | 13 | 6 | 16 | 9 | 2 | 12 | 5 | 15 | 8 | 1 | 11 | 4 | 14 | 7 |
| 11 | 11 | 5 | 16 | 10 | 4 | 15 | 9 | 3 | 14 | 8 | 2 | 13 | 7 | 1 | 12 | 6 |
| 12 | 12 | 7 | 2 | 14 | 9 | 4 | 16 | 11 | 6 | 1 | 13 | 8 | 3 | 15 | 10 | 5 |
| 13 | 13 | 9 | 5 | 1 | 14 | 10 | 6 | 2 | 15 | 11 | 7 | 3 | 16 | 12 | 8 | 4 |
| 14 | 14 | 11 | 8 | 5 | 2 | 16 | 13 | 10 | 7 | 4 | 1 | 15 | 12 | 9 | 6 | 3 |
| 15 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |
| 16 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

|  |  |
| --- | --- |
| **N** | **Inv.** |
| **1** | **1** |
| **2** | **9** |
| **3** | **6** |
| **4** | **13** |
| **5** | **7** |
| **6** | **3** |
| **7** | **5** |
| **8** | **15** |
| **9** | **2** |
| **10** | **12** |
| **11** | **14** |
| **12** | **10** |
| **13** | **4** |
| **14** | **11** |
| **15** | **8** |
| **16** | **16** |

Fermat theorem

If m prime, 1 (mod m)

m = 17, a = 2, 1 (mod 17)

xxx (mod17)

(-1)x(-1)x(-1)x(-1) (mod17)

1 (mod 17)

m =17, a = 3,  1 (mod 17)

xxxxxx (mod 17)

(-2)x(-2)x(-2)x(-2)x(-2)x(-2)x(-2)x(-2) (mod 17)

16 x 16 (mod17)

(-1) x (-1) (mod17)

1 (mod17)

Composite number: 16

Multiplication table for B =16

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 |
| 3 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 27 | 30 | 33 | 36 | 39 | 42 | 45 |
| 4 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60 |
| 5 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 | 55 | 60 | 65 | 70 | 75 |
| 6 | 6 | 12 | 18 | 24 | 30 | 36 | 42 | 48 | 54 | 60 | 66 | 72 | 78 | 84 | 90 |
| 7 | 7 | 14 | 21 | 28 | 35 | 42 | 49 | 56 | 63 | 70 | 77 | 84 | 91 | 98 | 105 |
| 8 | 8 | 16 | 24 | 32 | 40 | 48 | 56 | 64 | 72 | 80 | 88 | 96 | 104 | 112 | 120 |
| 9 | 9 | 18 | 27 | 36 | 45 | 54 | 63 | 72 | 81 | 90 | 99 | 108 | 117 | 126 | 135 |
| 10 | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 | 110 | 120 | 130 | 140 | 150 |
| 11 | 11 | 22 | 33 | 44 | 55 | 66 | 77 | 88 | 99 | 110 | 121 | 132 | 143 | 154 | 165 |
| 12 | 12 | 24 | 36 | 48 | 60 | 72 | 84 | 96 | 108 | 120 | 132 | 144 | 156 | 168 | 180 |
| 13 | 13 | 26 | 39 | 52 | 65 | 78 | 91 | 104 | 117 | 130 | 143 | 156 | 169 | 182 | 195 |
| 14 | 14 | 28 | 42 | 56 | 70 | 84 | 98 | 112 | 126 | 140 | 154 | 168 | 182 | 196 | 210 |
| 15 | 15 | 30 | 45 | 60 | 75 | 90 | 105 | 120 | 135 | 150 | 165 | 180 | 195 | 210 | 225 |

Multiply modulo 16

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 |
| 3 | 3 | 6 | 9 | 12 | 15 | 2 | 5 | 8 | 11 | 14 | 1 | 4 | 7 | 10 | 13 |
| 4 | 4 | 8 | 12 | 0 | 4 | 8 | 12 | 0 | 4 | 8 | 12 | 0 | 4 | 8 | 12 |
| 5 | 5 | 10 | 15 | 4 | 9 | 14 | 3 | 8 | 13 | 2 | 7 | 12 | 1 | 6 | 11 |
| 6 | 6 | 12 | 2 | 8 | 14 | 4 | 10 | 0 | 6 | 12 | 2 | 8 | 14 | 4 | 10 |
| 7 | 7 | 14 | 5 | 12 | 3 | 10 | 1 | 8 | 15 | 6 | 13 | 4 | 11 | 2 | 9 |
| 8 | 8 | 0 | 8 | 0 | 8 | 0 | 8 | 0 | 8 | 0 | 8 | 0 | 8 | 0 | 8 |
| 9 | 9 | 2 | 11 | 4 | 13 | 6 | 15 | 8 | 1 | 10 | 3 | 12 | 5 | 14 | 7 |
| 10 | 10 | 4 | 14 | 8 | 2 | 12 | 6 | 0 | 10 | 4 | 14 | 8 | 2 | 12 | 6 |
| 11 | 11 | 6 | 1 | 12 | 7 | 2 | 13 | 8 | 3 | 14 | 9 | 4 | 15 | 10 | 5 |
| 12 | 12 | 8 | 4 | 0 | 12 | 8 | 4 | 0 | 12 | 8 | 4 | 0 | 12 | 8 | 4 |
| 13 | 13 | 10 | 7 | 4 | 1 | 14 | 11 | 8 | 5 | 2 | 15 | 12 | 9 | 6 | 3 |
| 14 | 14 | 12 | 10 | 8 | 6 | 4 | 2 | 0 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |
| 15 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Co-primes of B(16) are: **1, 3, 5, 7, 9, 11, 13, 15**

Euler parameter:8

|  |  |
| --- | --- |
| N | Inv |
| 1 | 1 |
| 3 | 11 |
| 5 | 13 |
| 7 | 7 |
| 9 | 9 |
| 11 | 3 |
| 13 | 5 |
| 15 | 15 |

Euler theorem:

If m and a co-primers: 1 mod m

is Eular coefficient

b = 15, m =16, = 8

15x15x15x15x15x15x15x15 (mod 16)

(-1)x(-1)x(-1)x(-1)x(-1)x(-1)x(-1)x(-1) (mod 16)

1 (mod 15)

b=5, m = 16, = 8

25x25x25x25 (mod 16)

9x9x9x9 (mod 16)

(-7)x(-7)x(-7)x(-7) (mod 16)

49x49 (mod 16)

1x1 (mod 16)