CS 4823: Homework #3

Due on February 9, 2018

Christopher Tse

Problem 1

Solve $122x \equiv 3(mod\ 343)$. Show step-by-step calculations.

Solution

Finding GCD
Using Euclidean Division Algorithm:

$$\begin{aligned} 343 &= 122(2) + 99 \\ 122 &= 99(1) + 23 \\ 99 &= 23(4) + 7 \\ 23 &= 7(3) + 2 \\ 7 &= 2(3) + 1 \end{aligned}$$

Follow with Extended Euclidean Algorithm:

$$\begin{aligned} 1 &= 7 + 2(-3) \\ &= 7 + (23 + 7(-3))(-3) = 7(10) + 23(-3) \\ &= (99 + 23(-4))(10) + 23(-3) = 99(10) + 23(-43) \\ &= 99(10) + (122 + 99(-1))(-43) = 99(53) + 122(-43) \\ &= (343 + 122(-2))(53) + 122(-43) \\ 1 &= 343(53) + 122(-149) \end{aligned}$$

In the case of $122x \equiv 1(mod\ 343)$ we have $x = -149 \equiv 194(mod\ 343)$, so for $122x \equiv 3(mod\ 343)$ we have $x = 194 * 3(mod\ 343) = 239$

Problem 2

a) Is your ID number invertible modulo $m = 2^{64}$?

ID = 112971666, since $gcd(ID, 2^{64}) = 2$, there is no inverse.

b) Let a be the least integer that is no less than your ID number and is invertible mod m. Use Sage xgcd to find the inverse of $a \ mod \ m$.

```
sage: a = 112971667
sage: g,x,y = xgcd(a, 2**64)
sage: print(g,x,y)
(1, -3514066771570022757, 21520870)
```

From the above output from Sage, we can see that $1 = a(-3514066771570022757) + 2^{64}(21520870)$. Therefore, inverse of a is -3514066771570022757.

c) In a C++ program, assume that there is a variable x with type ”unsigned long int” (64bits), and the product of a and x is 2018, what is x?

```
// main.cpp
#include <iostream>

using namespace std;

int main() {
    unsigned long int a = 112971666;
    cout << a / 2018 << endl;
    return 0;
}

// bash output
$ make main
c++     main.cpp   -o main
$ ./main
55981
```

Problem 3

Determine the unit group and the zero divisors of the ring $\mathbb{Z}/16\mathbb{Z}$.

Unit Group

Unit group is the set of elements in $16\mathbb{Z}$ where $a_i \in \mathbb{Z}$ and $gcd(a_i, 16) = 1$. Therefore: $\{1, 3, 5, 7, 9, 11, 13, 15\}$

Zero Divisors

Zero divisors is the set of elements in $16\mathbb{Z}$ where $a_i \in \mathbb{Z}$ and $gcd(a_i, 16) \neq 1$. Therefore: $\{2, 4, 6, 8, 10, 12, 14\}$

Problem 4

Determine the unit group and the zero divisors of the ring $\mathbb{Z}/15\mathbb{Z}$.

Unit Group

Unit group is the set of elements in $15\mathbb{Z}$ where $a_i \in \mathbb{Z}$ and $gcd(a_i, 15) = 1$. Therefore: $\{1, 2, 4, 7, 8, 11, 13, 14\}$

Zero Divisors

Zero divisors is the set of elements in $15\mathbb{Z}$ where $a_i \in \mathbb{Z}$ and $gcd(a_i, 15) \neq 1$. Therefore: $\{3, 5, 6, 9, 10, 12\}$