Lecture 21: Modular Arithmetic Handout Notes

Interesting Things About Modular Arithmetic

State 3 of them:

The operations we will study in the modular world:

 1.

 2.

 3.

 4.

 5.

 6.

 7.

Outline

SECTION 1:	COMPLEXITY OF OPERATIONS IN INTEGERS
SECTION 2:	MODULAR ARITHMETIC: BASIC DEFINITIONS AND PROPERTIES
SECTION 3:	COMPLEXITY OF OPERATIONS MODULO N

1 COMPLEXITY OF OPERATIONS IN INTEGERS

	Poly-time?	${f Algorithm}$	Additional notes
Addition			
Subtraction			
Multiplication			
Division			
Exponentiation			
Taking roots			
Taking logs			
Factorization	Don't know	Best one is exponential time	Want it to be computationally hard for cyrpto
isPrime	Yes	Miller-Rabin Monte Carlo alg.	A poly-time deterministic algorithm is also known
$\begin{array}{c} \mathbf{Generating} \\ n\text{-bit prime} \end{array}$	Yes	Random sampling + isPrime	No poly-time deterministic algorithm is known

2 MODULAR ARITHMETIC: BASIC DEFINITIONS AND PROPERTIES

Notation: "A is congruent to B modulo N":

Fact/Exercise: $A \equiv_N B$ if and only if N divides A - B.

Notation: $\mathbb{Z}_N =$

2.1 Addition

Definition ["plus" in \mathbb{Z}_N]:

Addition table for \mathbb{Z}_5

+	0	I	2	3	4
0					
I					
2					
3					
4					

What is the *additive identity*?

2.2 Subtraction

Definition ["additive inverse" in \mathbb{Z}_N]:

Definition ["minus" in \mathbb{Z}_N]:

For every $A \in \mathbb{Z}_N$, -A exists (why?)

 \Longrightarrow

Every row of the addition table of \mathbb{Z}_N is a permutation of \mathbb{Z}_N .

2.3 Multiplication

Definition ["multiplication" in \mathbb{Z}_N]:

Multiplication table for \mathbb{Z}_5



What is the *multiplicative identity*?

2.4 Division

Definition ["multiplicative inverse" in \mathbb{Z}_N]:

Definition ["division" in \mathbb{Z}_N]:

Is it true that for every $A \in \mathbb{Z}_N$, A^{-1} exists?

In \mathbb{Z}_6 , which elements have a multiplicative inverse?

Fact: $A^{-1} \in \mathbb{Z}_N$ exists if and only if

Definition: $\mathbb{Z}_N^* =$

Definition: $\varphi(N) =$

Multiplication table for \mathbb{Z}_8^*

•		3	5	7
L	-	З	5	7
3	3	Ι	7	5
5	5	7	Ι	3
7	7	5	3	

For every $A \in \mathbb{Z}_N^*$, A^{-1} exists

```
\implies
```

Every row of the multiplication table of \mathbb{Z}_N^* is a permutation of \mathbb{Z}_N^* .

2.5 Exponentiation (in particular in \mathbb{Z}_N^*)

Notation: For $A \in \mathbb{Z}_N, E \in \mathbb{N}, A^E =$

What is a **generator** in \mathbb{Z}_N^* ?

Theorem [Euler's Theorem]:

What is Fermat's Little Theorem?

IMPORTANT NOTE:

When exponentiating elements in \mathbb{Z}_N^* ,

COMPLEXITY OF OPERATIONS MODULO N

	Poly-time?	${f Algorithm}$	Additional notes
Addition			
Subtraction			
Multiplication			
Division			
Exponentiation			
Taking roots			
Taking logs			

Additional notes for division (computing B^{-1}):