

# CSCI 5421 - Homework 2

## Kelsey Neis, neis@umn.edu

### 31.1 6

Prove if  $p$  is prime and  $0 < k < p$ , then  $p \mid \binom{p}{k}$

conclude:

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

$$\begin{aligned}
 (a+b)^p &\equiv a^p + b^p \pmod{p} \\
 \text{iff } p &\mid (a+b)^p - (a^p + b^p) \\
 (a+b)^p &= \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k = \binom{p}{0} a^p b^0 + \binom{p}{p} a^0 b^p + \sum_{k=1}^{p-1} \binom{p-1}{k} a^{p-k-1} b^{k+1} \\
 (a+b)^p - (a^p + b^p) &= \sum_{k=1}^{p-1} \binom{p-1}{k} a^{p-k-1} b^{k+1} \\
 \frac{\binom{p}{k}}{p} &= \frac{(p-1)!}{k!(p-1-k)!} \cdot p = \binom{p-1}{k} \cdot p \\
 &\quad \text{binomial Coeff} \times p
 \end{aligned}$$

$a \equiv b \pmod{n}$  iff  $n \mid (a-b)$   
 equivalence relation (mod n)

## 7

1. Prove if  $a$  and  $b$  are positive integers such that  $a \mid b$ , then  $(X \bmod b) \bmod a = X \bmod a$  for any  $X$
2. prove  $X \equiv y \pmod{b}$  implies  $X \equiv y \pmod{a}$  for any  $x$  and  $y$

$$\textcircled{1} \quad a \mid b \text{ implies } m \cdot a = b \quad \text{so } (X \bmod b) \bmod a = x \bmod a \\ = (X \bmod m \cdot a) \bmod a = x \bmod a$$

$$\text{Case 1: } b < X \rightarrow m \cdot a < X \\ X = q \cdot b + r = \underbrace{q \cdot m \cdot a}_{\text{some factor of } a} + r \Rightarrow r' = (q \cdot m \cdot a + r) \bmod a \\ r' = r$$

$$\text{Case 2: } b > X \rightarrow m \cdot a > X \\ r = X \rightarrow X \bmod b = X \\ (X \bmod b) \bmod a = X \bmod a$$

$$\textcircled{2} \quad X \equiv y \pmod{b} \rightarrow X \equiv y \pmod{a} \quad (\text{given } a \mid b)$$

$$\hookrightarrow X \equiv y \pmod{m \cdot a} \rightarrow X \equiv y \pmod{a}$$

$$m \cdot a \mid X - y \quad \text{if } X \equiv y \pmod{b}, \text{ then their difference is divisible by } b \\ \text{implies } a \mid X - y, \text{ so } X \equiv y \pmod{a}$$

## 8

- for any  $k > 0$ ,  $n$  is a  $k$ th power if there exists  $a$  such that  $a^k = n$
- $n > 1$  is a non-trivial power if it is a  $k$ th power for  $k > 1$
- Show how to determine whether a  $\beta$ -bit integer  $n$  is a nontrivial power in time polynomial in  $\beta$

$$a^k = n, \quad n > 1, \quad k > 1$$

$a = 2$   
 $k = 0$   
 while  $a < \log_2 n$  —  $\beta$   
      $k = \log_a n$   
     if  $k \in \mathbb{Z}$  and  $k > 1$  then return true  
      $a++$

if  $\log_{\text{base } a} \text{ of } n$   
 is an integer, then  
 $n$  is a non-trivial power.

$\log_2 n$  is the ceiling for the checks needed to determine whether  $n$  is a non-trivial power, because 2 is the smallest non-trivial power.

## 31.2

### 3

prove that for all integers  $a, k, n$ ,  $\gcd(a, n) = \gcd(a + kn, n)$

Euclid:

$$a \quad n \quad \left( \begin{array}{c} a \bmod n \\ n \bmod a \bmod n \dots \end{array} \right)$$

$$a + kn \quad n \quad \left( \begin{array}{c} a + kn \bmod n \\ \underbrace{\hspace{1cm}} \\ a \bmod n \end{array} \right) \quad n \bmod a \bmod n \dots$$

Following Euclid's method of finding the gcd, we see that  **$a + kn \bmod n$**  simplifies down to  **$a \bmod n$** , because  **$kn$**  is  **$0 \bmod n$** . In other words,  **$a + kn$**  is equivalent to  **$a \pmod n$** .

4

```
Euclid(a, b)
1 while b ≠ 0
2   { a = b
3     b = a mod b
4   }
5 return a
```

Writing over the variables  $a$  and  $b$  means this will only store those 2 variables.

## 6

Since the sequence of Fibonacci numbers starts with 0, 1, 1 is the gcd of any adjacent Fibonacci numbers. So, the first  $d'$ ,  $x'$ ,  $y'$  triple would be  $d' = 1$ ,  $x' = 1$ ,  $y' = 0$ . Interestingly,  $x$  and  $y$  follow a sort of Fibonacci sequence as well, alternating positive and negative

working back- wards ↓	a	b	$\lfloor a/b \rfloor$	d	x	y
	1	0	return	1	1	0
	2	1	1	1	0	1
	3	2	1	1	1	-1
	5	3	1	1	-1	2
	8	5	1	1	2	-3
	13	8	1	1	-3	5
	⋮	⋮	⋮	⋮	⋮	⋮
	$F_{k+1}$	$F_k$	1	1		

$x = y'$   
 $y = x' - \lfloor a/b \rfloor y'$   
*always = 1 in Fib. sequence*

*b/c sign flipped to negative, this pattern continues*

*-  $x'$  &  $y'$  have opposite signs, so  $x' - y'$  will increase  $|y|$  by  $x'$ , leading to a Fibonacci sequence*

$$d = 1, \quad x = (-1)^{(k+1)\%2} \cdot F_{k-2}, \quad y = (-1)^{k\%2} \cdot F_{k-1}$$

Because  $\text{floor}(a/b)$  is always one for the fibonacci sequence, the  $x$  and  $y$  values are a result of summing up previous  $x$  and  $y$  values, forming another Fibonacci sequence, which is 3 behind for **a** and 2 behind for **b**. Assuming  $F_1$  is the first row in the table,  $x$  is negative on the even indexes and  $y$  is negative on the odd indexes, hence  $(-1)^{k+1\%2}$  and  $(-1)^{k\%2}$

## 31.3

# 1

$$\begin{array}{l}
 (\mathbb{Z}_4, +_4): \\
 \{0, 1, 2, 3\}
 \end{array}
 \begin{array}{c|cccc}
 +_4 & 0 & 1 & 2 & 3 \\
 \hline
 0 & 0 & 1 & 2 & 3 \\
 1 & 1 & 2 & 3 & 0 \\
 2 & 2 & 3 & 0 & 1 \\
 3 & 3 & 0 & 1 & 2
 \end{array}
 \quad
 \begin{array}{l}
 (\mathbb{Z}_5^*, \cdot_5) \\
 \{1, 2, 3, 4\}
 \end{array}
 \begin{array}{c|cccc}
 \cdot_5 & 1 & 2 & 3 & 4 \\
 \hline
 1 & 1 & 2 & 3 & 4 \\
 2 & 2 & 4 & 1 & 3 \\
 3 & 3 & 1 & 4 & 2 \\
 4 & 4 & 3 & 2 & 1
 \end{array}$$

We need to find the order of  $\mathbb{Z}^*$  and we do this by finding the first instance of the identity, 1. Evidently, the order is 2, since 2, 3 is the first inverse pair. Where we look at the abelian group for  $2^x \bmod 5$  we see it is cyclic:

$$\begin{array}{c|ccccc}
 2^x_5 & 2^0 & 2^1 & 2^2 & 2^3 & 2^4 \\
 \hline
 & 1 & 2 & 4 & 3 & 1
 \end{array}$$

So, this is a good candidate for alpha

Plugging in  $a, b$ , where  $\alpha = 2^x$ :

$\mathbb{Z}_4$

$$0+0=0 \pmod 4$$

$$0+1=1 \pmod 4$$

$$0+2=2 \pmod 4$$

$$0+3=3 \pmod 4$$

$a \quad b \quad c$

$\mathbb{Z}_5^*$

$$2^0 \cdot 2^0 = 2^0 = 1 \pmod 5$$

$$2^0 \cdot 2^1 = 2^1 = 2 \pmod 5$$

$$2^0 \cdot 2^2 = 2^2 = 4 \pmod 5$$

$$2^0 \cdot 2^3 = 2^3 = 3 \pmod 5$$

$\begin{matrix} 1 & 1 & 1 \\ a & b & c \end{matrix}$

Assuming that the  $a, b$ , and  $c$  refer to the same number on both sides,  $x = 2^x$  and these groups are indeed isomorphic.

## 2

To generate subgroups, multiply  $a$  by each member of  $\mathbb{Z}$  until the end of the cycle mod  $n$

$\mathbb{Z}_9$ :  $a=0$ : identity, trivial set  $\{0\}$

$$a=1: \begin{array}{c|cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$a=2: \begin{array}{c|cccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 2 & 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \end{array} \quad \{0, 2, 4, 6, 8\}$$

$\mathbb{Z}_{13}^*$

$a=1$ :  $\{1\}$  — trivial identity set

$$a=2: \begin{array}{c|cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \hline 2 & 2 & 4 & 6 & 8 & 10 & 12 & 1 & 3 & 5 & 7 & 9 & 11 \end{array}$$

$$\hookrightarrow \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12\}$$

### 3

For  $S'$  to be a subgroup, it must be closed under the binary operation. Since that is part of the presupposition of the theorem, the first requirement is met. Secondly, there needs to be an identity. This also follows from the fact that  $S'$  is closed, because if it did not contain the identity, then it wouldn't be closed

suppose  $S' \subseteq S$  not containing  $e$

then there is no combination of  $a$  and  $b$

such that  $a \oplus b = e$

and yet,  $\forall a \oplus b \equiv e \pmod{n}$

Since the group is closed

It follows that  $S'$  is not closed if  $e$  is not in  $S'$ ,

a contradiction of  $a \oplus b \in S'$

Therefore, the identity is in  $S'$

$+$	$4$	$1$	$2$	$3$
$1$		$2$	$3$	$0$
$2$		$3$	$0$	$1$
$3$		$0$	$1$	$2$

example w/  $S'_4$   
w/o  $e$ .

$e$  shows up in the map and so must be part of  $S'$



The last requirement is that the operations must be associative. If  $S$  is an Abelian group, then the binary operations in  $S$  are associative. Since  $S'$  is a subset of  $S$ , it follows that  $S'$  meets this requirement.

## 4

show:  $\phi(p^e) = p^{e-1}(1-p)$

$$\phi(p^e) = p^e \prod_{p|p^e} \left(1 - \frac{1}{p}\right) \leftarrow \begin{array}{l} \text{there is only one } p \\ \text{which divides } p^e, \\ \text{because } p \text{ is prime} \\ \text{therefore, } (1 - \frac{1}{p}) \text{ is only} \\ \text{multiplied } \underline{\text{once}} \end{array}$$

$$\Rightarrow p^e \left(1 - \frac{1}{p}\right)$$

$$= p^e - \frac{p^e}{p}$$

$$= p^e - p^{e-1}$$

$$= \underline{p^{e-1}(1-p)}$$

## 5

If  $Z^*$  is closed under a binary operation, then performing that operation against all members

of the group for any  $a \in \mathbb{Z}^*$  will yield numbers within that group.

How can we be sure the resulting group is distinct?

By the property of Abelian groups that the map of the binary operation for It has no zero divisors. Therefore, every distinct number mapped by  $f(x)$  yields a distinct number mod  $n$ .

It follows from the fact that the group is closed and only yields distinct values from binary operations that  $f(x)$  will result in a permutation of  $\mathbb{Z}^*$