Math 458, Exam 1
Spring 2019
Instructor: Dugger

Name: Solutions

Instructions: This is a 50 minute exam. You are allowed a 3×5 notecard (front and back) and a calculator. Answers must be accompanied by explanations to earn full credit.

1. (10 points) Solve the equation $5x + 17 = 1$ in $\mathbb{F}_{29}$.

$5x = 1 - 17 = -16 = 13$

Need 5^{-1} ⟶

$1 \equiv 30 = 5 \cdot 6 \mod 29$

So $6 = 5^{-1}$

$x = 13 \cdot 5^{-1} = 13 \cdot 6 = 78$

$= 20$ in $\mathbb{F}_{29}$

$\boxed{x = 20}$

2. (10 points) Is it true that $\sin^2(x) = \mathcal{O}(x)$? Justify your answer.

$\sin^2(x) \leq 1 \leq 1 \cdot x$ when $x \geq 1$

So yes.

One can make a case that $x \geq 0$ is enough, but that takes more work

3. (10 points) Alice and Bob are using the ElGamal system to send messages. Because they only need to keep their messsages secure from Alice's three-year-old brother Michael, it is safe for them to use the prime $p = 7$ with primitive root $g = 3$. Alice's public key is $A = 2$. Bob encrypts a secret number $m \in \{0, 1, \ldots, 6\}$ and sends the ciphertext to Alice: Alice receives the message $(5, 2)$. She shows it to Michael and says, "You don't know what the secret number is, ha ha!" But Michael is just dying to know.

   Help Michael find the secret number. Show all your steps and explain your reasoning (briefly).

$m = (c_1^a)^{-1} \cdot c_2$ So need a.

$2 = A = 3^a$ $3^0 = 1$, $3^1 = 3$, $3^2 = 9 = 2$ So $a = 2$

$m = (5^2)^{-1} \cdot 2 = (25)^{-1} \cdot 2 = 4^{-1} \cdot 2$

$4 \cdot 2 = 8 = 1$
So $2 = 4^{-1}$

$= 2 \cdot 2$
$= 4$

$\boxed{m = 4}$

4. (10 points) Find the inverse of 35 in $\mathbb{Z}/221$.

$$\begin{array}{r} 6 \\ 35 \overline{)\,221} \\ \underline{210} \\ 11 \end{array}$$

$221 = 35(6) + 11$
$35 = 11(3) + 2$
$11 = 2(5) + 1$

$\Rightarrow$

$1 = 11 - 2 \cdot 5$
$= 11 - (35 - 11 \cdot 3) \cdot 5$
$= 16 \cdot 11 - 5 \cdot 35$
$= 16(221 - 6 \cdot 35) - 5 \cdot 35$
$= 16 \cdot 221 - (16 \cdot 6 + 5) \cdot 35$
$= 16 \cdot 221 - 101 \cdot 35$

$\Leftarrow$

Mod 221 have $1 = -101 \cdot 35$

So $35^{-1} = -101 = 221 - 101 = \underline{120}$

$\boxed{35^{-1} = 120}$

5. (10 points) What is the remainder when 3^{12153} is divided by 101? Explain how this can be determined using only paper, pen, and a calculator that handles numbers up to 5 digits.

$3^{100} = 1$ and $12153 = 121 \cdot 100 + 53$

So $3^{12153} = (3^{100})^{121} \cdot 3^{53} = 1^{121} \cdot 3^{53} = 3^{53}$ (1)

(2) Easiest method is probably $3^{53} = 3^3 \cdot (3^{10})^5 = 3^3 ((3^5)^2)^5$

$3^5 = 243 = 41$

$(3^5)^2 = 41^2 = 1681 = 65$

$(65)^5 = 65 \cdot 65^2 \cdot 65^2 = 65 \cdot 84 \cdot 84$

$= 65 \cdot 87 = 100$

$3^{53} = 27 \cdot 100 = \underline{\underline{74}}$.

Can also use powers of 2, etc.

This problem was too long: but anyone who demonstrated (1) and some knowledge of fast powering got almost full credit.

6. (10 points) Alice and Bob are using the Diffie-Hellman key exchange method. They are using $p = 11$ with primitive root $g = 2$. Alice sends Bob her public key $A = 10$, and Bob sends Alice his public key $B = 7$. Since the prime p is very small, the Diffie-Hellman exchange is not very safe. Find the shared key, and also find Alice's secret number a.

$A = g^a = 2^a$ $B = g^b = 2^b$

$10 = 2^a$ So try brute force: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = \underline{\underline{10}}$

So $a = 5$

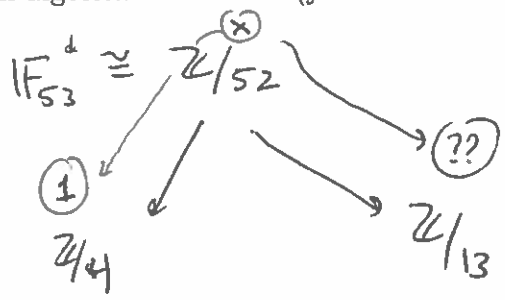
Shared key is $B^a = 7^5 = 16807 \equiv 10 \bmod 11$

Shared key = 10

7. (10 points) You want to solve $2^x = 20$ in $\mathbb{F}_{53}$. You are given the helpful information that $x \equiv 1 \pmod 4$ together with the following calculations of powers in $\mathbb{F}_{53}$:

$$46 = 7^{40} = 8^{48} = 16^{10} = 32^8 = 20^4 = 15^{38}.$$

Use the Pohlig-Hellmann algorithm to find x (you won't need all of the above information).



$52 = 2^2 \cdot 13$

Step 1: Find $x \bmod 13$

$2^x = 20 \Rightarrow (2^x)^4 = 20^4 \Rightarrow 16^x = 46$

Look at given information and see $x = 10$.

Step 2: Now do CRT: $x \equiv 1 \bmod 4$

$x \equiv 10 \bmod 13$

$x = 1 + 4n$, $n \in \mathbb{Z}$

$10 = x = 1 + 4n$ in $\mathbb{Z}/13$

$9 = 4n$ in $\mathbb{Z}/13$ Need 4^{-1}: $1 = 14 = 27 = \underline{40}$

So $4 \cdot 10 = 1$, or $4^{-1} = 10$.

$90 = 9 \cdot 10 = n \Rightarrow n = 90 = 12$ in $\mathbb{Z}/13$

$n = 12 + 13r$ for some $r \in \mathbb{Z}$

$x = 1 + 4(12 + 13r) = 1 + 48 + 52r = 49 + 52r$

$\boxed{x = 49}$

8. You want to solve $11^x = 2$ in $\mathbb{F}_{71}$. You are given the following tables of information:

i	0	1	2	3	4
11^i	1	11	50	53	15

i	0	1	2	3	4
11^{-5i}	1	34	20	41	45

(a) (10 points) Use the above information and the Shanks Baby-Step/Giant-Step Algorithm (with $n = 5$) to solve for x.

Need $2 \cdot 11^{-5i}$:

0	1	2	3	4
2	68	40	82 = 11	90 = 19

Have a match :

$$11^1 = 2 \cdot 11^{-5 \cdot 3}$$

$$11^1 = 2 \cdot 11^{-15}$$

$$11^1 \cdot 11^{15} = 2$$

$$11^{16} = 2$$

$$\boxed{x = 16}$$

(b) (5 points Extra Credit) Something might be bothering you about part (a), and in fact we got somewhat lucky that this worked out. Explain why.

We are only guaranteed a match if we use $n = \lfloor \sqrt{71} \rfloor + 1 = 8 + 1 = 9$.

So using $n = 5$ is risky, as we might not have a match.

But in this case we got lucky and did have one.