Exam 1 – Take home

Printed Name: Paul Beggs

Instructions: This is an individual, open-book, open-notes exam. You may not give help, receive help, or discuss this exam with anyone apart from me.

You may use a calculator or the computer to help with computations, just be sure to cite when you do so.

You may consult your textbook, your personal class notes, and your previous homework assignments while working on this exam. You may also consult anything posted on our Teams page. Only these resources are allowed.

You may NOT consult any other sources. No internet sources. No other textbooks. No notes or any other material from other students. No consulting with another student. No consulting with another professor.

As always, show work to get full credit (the correct answer may NOT be enough).
Write clearly! Double check your answers!

Honor Pledge: I have neither received nor given aid on this work, nor have I witnessed any such violation of the Honor Code.

Honor Pledge Signature:

Question	Points	Score
1	10	
2	10	
3	10	
Total:	30	

1. Let a, b be positive integers and $D = \gcd(a, b)$. Prove that if $x^a \equiv 1 \pmod{m}$ and $x^b \equiv 1 \pmod{m}$ then $x^D \equiv 1 \pmod{m}$. [10]

Definitions to be used in the proof:

(a) **Divides:** For integers $a, b \in \mathbb{Z}$, we say that a divides b if there exists an integer c such that $b = ac$. Notated as $a \mid b$.

(b) **GCD:** The greatest common divisor of two integers a and b, denoted $D = \gcd(a, b)$, is the largest positive integer such that $D \mid a$ and $D \mid b$. This means there exists $p, q \in \mathbb{Z}$ such that $D = pa + qb$.

> *Proof.* Let a, b be positive integers and $D = \gcd(a, b)$, and suppose $x^a \equiv 1 \pmod{m}$ and $x^b \equiv 1 \pmod{m}$. Since $D = \gcd(a, b)$, we know that there exists $p, q \in \mathbb{Z}$ such that $D = pa + qb$ by the definition of GCD. Now, consider $x^D \equiv 1 \pmod{m}$. We can rewrite x^D as x^{pa+qb}, and apply the properties of exponents. This gives us $x^{pa+qb} = (x^a)^p \cdot (x^b)^q$. Since $x^a \equiv 1 \pmod{m}$ and $x^b \equiv 1 \pmod{m}$, we can substitute these values into the equation. This gives us $(x^a)^p \cdot (x^b)^q = 1^p \cdot 1^q = 1$. Therefore, $x^D \equiv 1 \pmod{m}$. □

2. Prove that the set $\mathbb{Q}$ of rational numbers is a ring under addition and multiplication. Remember that you are only allowed to assume knowledge of the properties of integers, so treat $\mathbb{Q}$ as the set $\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$. [10]

Proof. For the following, let $x = \frac{a}{b}$, $y = \frac{c}{d}$, and $z = \frac{e}{f}$ be rational numbers in $\mathbb{Q}$ such that $a, b, c, d, e, f \in \mathbb{Z}$ where $b, d, f \neq 0$. We want to show that the set $\mathbb{Q}$ of rational numbers is a ring under addition and multiplication. Thus, consider the following:

(a) **Additive Closure.**
Consider $\frac{ad+bc}{bd}$. Since $a, b, c, d \in \mathbb{Z}$, we know that $ad + bc \in \mathbb{Z}$ because integer addition is closed. Moreover, because $b, d \neq 0$, we know that $bd \neq 0$. Therefore, $\frac{ad+bc}{bd} \in \mathbb{Q}$. This shows that rational numbers are closed under addition.

(b) **Additive Associativity.**
Consider $(x+y)+z = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f+edb}{bdf}$ because we know that the integers possess distributivity we know that $\frac{(ad+bc)f+edb}{bdf} = \frac{adf+bcf+cdb}{bdf}$. Similarly, consider $x + (y+z) = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+ed}{df} = \frac{a(df)+(cf+ed)b}{bdf} = \frac{adf+cbf+ebd}{bdf}$. By substitution, we can see that $(x + y) + z = x + (y + z)$. This shows that rational numbers are associative under addition.

(c) **Additive Commutativity.**
Consider $x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$. Then, consider $y + x = \frac{c}{d} + \frac{a}{b} = \frac{cb+ad}{db}$. Because addition is commutative in the integers, we know that $ad + cb = cb + ad$. Therefore, $x + y = y + x$. This shows that rational numbers are commutative under addition.

(d) **Additive Identity.**
Let $0 := \frac{0}{1}$. Consider $x + 0 = \frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b}$. This shows that the additive identity is 0.

(e) **Additive Inverse.**
Let $-x := \frac{-a}{b}$. Consider $x + (-x) = \frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + -a \cdot b}{b \cdot b} = \frac{0}{b^2} = 0$. This shows that the additive inverse is $-x$.

(f) **Multiplicative Closure.**
Consider $x \cdot y = \frac{ac}{bd}$. Since $a, b, c, d \in \mathbb{Z}$, we know that $ac \in \mathbb{Z}$ because integer multiplication is closed. Moreover, because $b, d \neq 0$, we know that $bd \neq 0$. Therefore, $\frac{ac}{bd} \in \mathbb{Q}$. This shows that rational numbers are closed under multiplication.

(g) **Multiplicative Associativity**
Consider $(x \cdot y) \cdot z = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf}$. Similarly, consider $x \cdot (y \cdot z) = \frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{ace}{bdf}$. By substitution, we can see that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. This shows that rational numbers are associative under multiplication.

(h) **Distributive Property.**
Consider $x \cdot (y+z) = \frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{cf+ed}{df} = \frac{acf+aed}{bdf}$. Similarly, consider $x \cdot y + x \cdot z = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acf+aed}{bdf}$. By substitution, we can see that $x \cdot (y+z) = x \cdot y + x \cdot z$. This shows that rational numbers are distributive under multiplication. □

3. The following is the full message that was encrypted using the monoalphabetic cipher mentioned on the in-class exam. Use Plot 1 and Plot 2 to decrypt the following message and include notes along the way on your thought process (why you made certain choices, why something did or did not seem to work, etc.) [10]

```
JMAVE EOMKE LEKEK VMREE NJMAV EEOMK ELEKE KVMRE
ENSNK VSOQM AXQMX NQQEK VMEKV MYKVS NLONE KDMAX
IOMKV MBXYM MXOBD IKDMA XIOMK VMBXY MVXYQ DMAXI
OMKVX KLEXP JSPPO MYHMK EEYLX NSZMX NQRMX DIYMK
VMDMO KEFEI YMNMY LSMOX NQOCS PPODM AXIOM KVXKA
VXPPM NLMSO ENMKV XKJMX YMJSP PSNLK EXAAM WKENM
JMXYM INJSP PSNLK EWEOK WENMX NQENM JVSAV JMSNK
MNQKE JSNXN QKVME KVMYO KEE
```

Solution.

(a) I substituted varying letters that are common in English for the most common letters in the ciphertext. For example, I substituted the letter `M` for the letter `E` since `M` is the most common letter in the ciphertext. I also substituted the letter `K` for the letter `T` since `V` is the second most common letter in the ciphertext. I continued this process until I got a string of letters that did not make sense together.

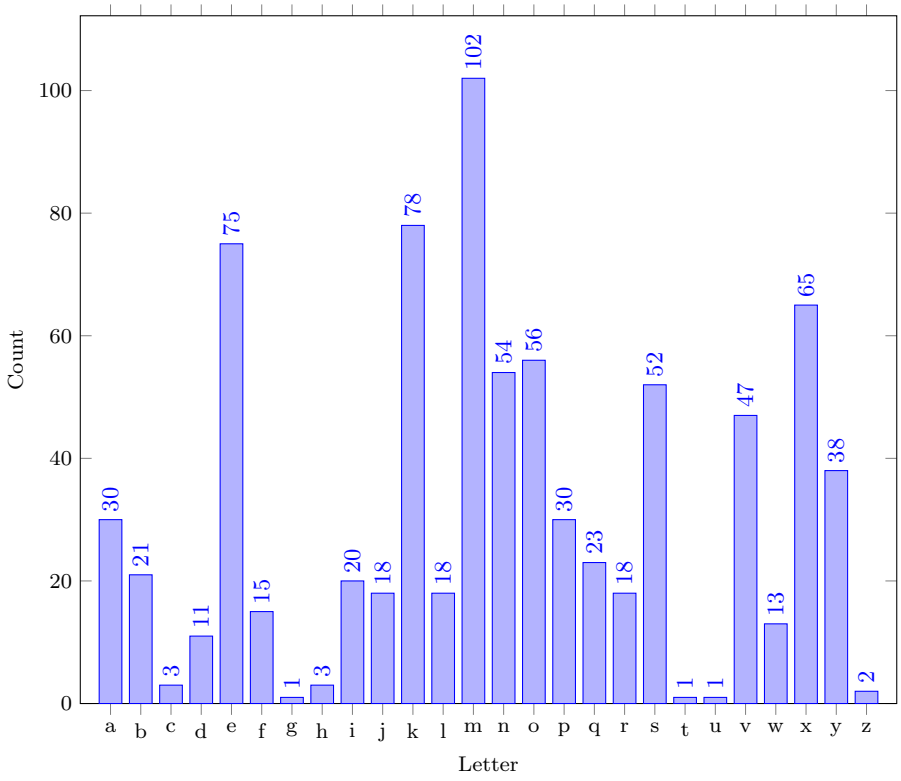
(b) When I would eventually run into problems with the mismatched string of characters, I would try to match letters that may fit into both the monogram frequency and the bigram frequency. This influenced my thoughts on whether `M` was `T` or `E`.

(c) Once most of the substitutions were made and there were still some characters that were out of place, I would reconsider a selection for a substitution that I made for one that made more sense.

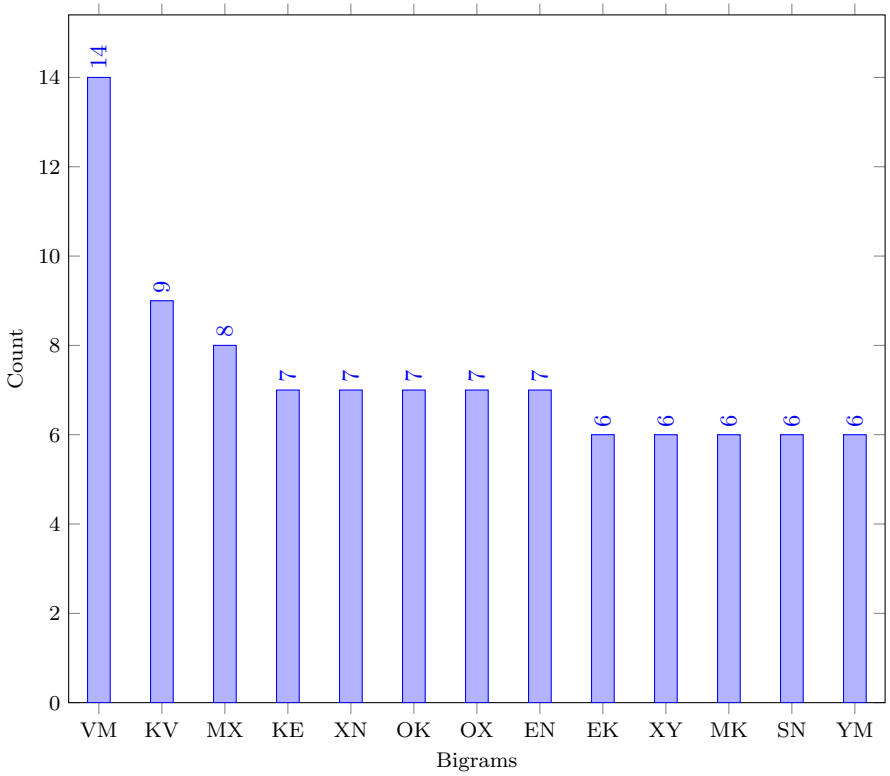
(d) I would iterate over this list until all the words made sense together.

Decrypted text:
We choose to go to the moon. We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win, and the others, too.

Plot 1: Frequency Analysis of Ciphertext (Unigram)



Plot 2: Frequency Analysis of Ciphertext (Bigrams)



Graph from this link.