Some Solutions to HW01 Problems
BILL, RECORD LECTURE!!!
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[
x^2 + 17x + 16 \equiv 0 \pmod{100}
\]
Problem 2

How many $x \in \{0, \ldots, 99\}$ satisfy the equation

$$x^2 + 17x + 16 \equiv 0 \pmod{100}$$

Wrong Answer: Its an equation of degree 2, so 2 solutions.
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[ x^2 + 17x + 16 \equiv 0 \pmod{100} \]

**Wrong Answer** Its an equation of degree 2, so 2 solutions.

**Key** If solving over \( \mathbb{R} \) or \( \mathbb{C} \) would do

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[
x^2 + 17x + 16 \equiv 0 \pmod{100}
\]

Wrong Answer Its an equation of degree 2, so 2 solutions.

Key If solving over \( \mathbb{R} \) or \( \mathbb{C} \) would do

\[
x^2 + 17x + 16 = (x + 16)(x + 1)
\]

If \( (x + 16)(x + 1) = 0 \) then EITHER \( x + 16 = 0 \) or \( x + 1 = 0 \).
Problem 2

How many $x \in \{0, \ldots, 99\}$ satisfy the equation

$$x^2 + 17x + 16 \equiv 0 \pmod{100}$$

**Wrong Answer** Its an equation of degree 2, so 2 solutions.

**Key** If solving over $\mathbb{R}$ or $\mathbb{C}$ would do

$$x^2 + 17x + 16 = (x + 16)(x + 1)$$

If $(x + 16)(x + 1) = 0$ then EITHER $x + 16 = 0$ or $x + 1 = 0$.

That does not apply in mod 100.

**Note** $25 \times 4 \equiv 0$, but $25 \neq 0$ and $4 \neq 0$. 
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[
x^2 + 17x + 16 \equiv 0 \pmod{100}
\]

Wrong Answer: It's an equation of degree 2, so 2 solutions.

Key: If solving over \( \mathbb{R} \) or \( \mathbb{C} \) would do

\[
x^2 + 17x + 16 = (x + 16)(x + 1)
\]

If \((x + 16)(x + 1) = 0\) then EITHER \(x + 16 = 0\) or \(x + 1 = 0\).

That does not apply in mod 100.

Note: \(25 \times 4 \equiv 0\), but \(25 \neq 0\) and \(4 \neq 0\).

Two ways to solve.
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[ x^2 + 17x + 16 \equiv 0 \pmod{100} \]

Wrong Answer: It's an equation of degree 2, so 2 solutions.

Key: If solving over \( \mathbb{R} \) or \( \mathbb{C} \) would do

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]

If \( (x + 16)(x + 1) = 0 \) then EITHER \( x + 16 = 0 \) or \( x + 1 = 0 \).

That does not apply in mod 100.

Note: \( 25 \times 4 \equiv 0 \), but \( 25 \neq 0 \) and \( 4 \neq 0 \).

Two ways to solve.
1) Write a program that goes through all \( x \in \{0, \ldots, 99\} \).
Problem 2

How many \( x \in \{0, \ldots, 99\} \) satisfy the equation

\[ x^2 + 17x + 16 \equiv 0 \pmod{100} \]

**Wrong Answer** Its an equation of degree 2, so 2 solutions.

**Key** If solving over \( \mathbb{R} \) or \( \mathbb{C} \) would do

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]

If \((x + 16)(x + 1) = 0\) then EITHER \(x + 16 = 0\) or \(x + 1 = 0\).

That does not apply in mod 100.

**Note** \(25 \times 4 \equiv 0\), but \(25 \neq 0\) and \(4 \neq 0\).

Two ways to solve.

1) Write a program that goes through all \( x \in \{0, \ldots, 99\} \).
2) By hand and cleverness on next slide.
Problem 2: The Clever Solutions, Mod 5

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]

**Lemma** \((x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \equiv 0 \pmod{5} \).
Problem 2: The Clever Solutions, Mod 5

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]

**Lemma** \((x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \equiv 0 \pmod{5}.\)

**Proof** \(x + 1 \not\equiv 0 \pmod{5} \implies x + 16 \not\equiv 0 \pmod{5} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{5} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100}.\)
Problem 2: The Clever Solutions, Mod 5

\[ x^2 + 17x + 16 = (x + 16)(x + 1) \]

**Lemma** \((x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \equiv 0 \pmod{5} \).

**Proof** \(x + 1 \not\equiv 0 \pmod{5} \implies x + 16 \not\equiv 0 \pmod{5} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{5} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100} \).

**Upshot** Only need to look \(x\) such that \(x + 1 \equiv 0 \pmod{5} \).

**Upshot** Only need to look at \(x \equiv 0 \pmod{5} \).
Problem 2: The Clever Solutions, Mod 4

Lemma \((x + 1)(x + 16) \equiv 0 \implies x + 1 \not\equiv 2 \pmod{4}\).
Problem 2: The Clever Solutions, Mod 4

**Lemma** \((x + 1)(x + 16) \equiv 0 \implies x + 1 \not\equiv 2 \pmod{4}\).

**Proof** \(x + 1 \equiv 2 \pmod{4} \implies x + 16 \equiv 1 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100}\).

**Upshot** Only need to look at \(x\) such that \(x + 1 \equiv 0, 1 \pmod{4}\).
Lemma $(x + 1)(x + 16) \equiv 0 \implies x + 1 \not\equiv 2 \pmod{4}$.

Proof $x + 1 \equiv 2 \pmod{4} \implies x + 16 \equiv 1 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100}$.

Lemma $(x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \not\equiv 3 \pmod{4}$. 
Problem 2: The Clever Solutions, Mod 4

**Lemma** \((x + 1)(x + 16) \equiv 0 \implies x + 1 \not\equiv 2 \pmod{4} \).  

**Proof** \(x + 1 \equiv 2 \pmod{4} \implies x + 16 \equiv 1 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100} \).  

**Lemma** \((x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \not\equiv 3 \pmod{4} \).  

**Proof** \(x + 1 \equiv 3 \pmod{4} \implies x + 16 \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100} \).  

\[ \]
Problem 2: The Clever Solutions, Mod 4

Lemma \((x + 1)(x + 16) \equiv 0 \implies x + 1 \not\equiv 2 \pmod{4}\).

Proof \(x + 1 \equiv 2 \pmod{4} \implies x + 16 \equiv 1 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100}\).

Lemma \((x + 1)(x + 16) \equiv 0 \pmod{100} \implies x + 1 \not\equiv 3 \pmod{4}\).

Proof \(x + 1 \equiv 3 \pmod{4} \implies x + 16 \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \equiv 2 \pmod{4} \implies (x + 1)(x + 16) \not\equiv 0 \pmod{100}\).

Upshot Only need to look at \(x\) such that \(x + 1 \equiv 0, 1 \pmod{4}\).

Upshot Only need to look at \(x \equiv 0, 3 \pmod{4}\).
Problem 2. Clever Sol Cont.

1) \( x \equiv 4 \pmod{5} \) and \( x \equiv 0 \pmod{4} \) implies \( x \equiv 4 \pmod{20} \).

\[
\begin{array}{|c|c|c|}
\hline
x & (x + 1)(x + 16) & \equiv 0 \pmod{100} \\ Y \\
\hline
4 & 100 & Y \\
24 & 1000 & Y \\
44 & 2700 & Y \\
64 & 5200 & Y \\
84 & 8400 & Y \\
\hline
\end{array}
\]

2) \( x \equiv 4 \pmod{5} \) and \( x \equiv 3 \pmod{4} \) implies \( x \equiv 19 \pmod{20} \).

\[
\begin{array}{|c|c|c|}
\hline
x & (x + 1)(x + 16) & \equiv 0 \pmod{100} \\ Y \\
\hline
19 & 700 & Y \\
39 & 2200 & Y \\
59 & 4500 & Y \\
79 & 7600 & Y \\
99 & 8400 & Y \\
\hline
\end{array}
\]

So there are 10 solutions.
Problem 2: The Point

**Point of the Problem** Mod 100 is very different than \( \mathbb{N} \) or \( \mathbb{Z} \) or even Mod 7 since you can have \( d \)th degree poly with MORE THAN \( d \) roots.
Problem 2: The Point

**Point of the Problem** Mod 100 is very different than \( \mathbb{N} \) or \( \mathbb{Z} \) or even Mod 7 since you can have \( d \)th degree poly with MORE THAN \( d \) roots.

**Theorem** If the domain is \( \mathbb{Z} \) or \( \mathbb{R} \) or \( \mathbb{C} \) (the complex numbers) then every poly of degree \( d \) has \( \leq d \) roots.
Point of the Problem: Mod 100 is very different than $\mathbb{N}$ or $\mathbb{Z}$ or even Mod 7 since you can have $d$th degree poly with MORE THAN $d$ roots.

**Theorem** If the domain is $\mathbb{Z}$ or $\mathbb{R}$ or $\mathbb{C}$ (the complex numbers) then every poly of degree $d$ has $\leq d$ roots.

The proof of this theorem used that in these domains

$$ab = 0 \implies (a = 0) \lor (b = 0)$$
Problem 4a

How many $a, b \in \{0, \ldots, 29\}$ are cool relative to 30.
How many $a, b \in \{0, \ldots, 29\}$ are cool relative to 30.

The numbers rel prime to 30 are $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Hence there are 8 of these.
How many $a, b \in \{0, \ldots, 29\}$ are cool relative to 30.

The numbers rel prime to 30 are $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Hence there are 8 of these.

The number of $b$’s is ALL of them: 30.
Problem 4a

How many $a, b \in \{0, \ldots, 29\}$ are cool relative to 30.

The numbers rel prime to 30 are $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Hence there are 8 of these.

The number of $b$’s is ALL of them: 30.

Hence there are $8 \times 30 = 240$ cool pairs.
A student picks an $a, b \in \{0, \ldots, 29\}$ at random. What is the probability that $(a, b)$ is cool relative to 30?
Problem 4b

A student picks an $a, b \in \{0 \ldots, 29\}$ at random. What is the probability that $(a, b)$ is cool relative to 30?

\[
\frac{240}{30 \times 30} = \frac{8 \times 30}{30 \times 30} = \frac{8}{30} = \frac{4}{15} \approx 0.2667
\]
Problem 4c

How many \((a, b)\) are cool relative to 31?
Problem 4c

How many \((a, b)\) are cool relative to 31?

The numbers rel prime to 31 are \(\{1, \ldots, 30\}\). Hence there are 30 of these.
Problem 4c

How many \((a, b)\) are cool relative to 31?

The numbers rel prime to 31 are \(\{1, \ldots, 30\}\). Hence there are 30 of these.

The number of \(b\)'s is ALL of them: 31.
Problem 4c

How many \((a, b)\) are cool relative to 31?

The numbers rel prime to 31 are \(\{1, \ldots, 30\}\). Hence there are 30 of these.

The number of \(b\)'s is ALL of them: 31.

Hence there are \(30 \times 31 = 930\) cool pairs.
A student picks an \( a, b \in \{0 \ldots, 30\} \) at random. What is the probability that \((a, b)\) is cool rel to 31? Give the answer to four decimal places.

\[
\frac{930}{31 \times 31} = \frac{30 \times 31}{31 \times 31} = \frac{30}{31} \approx 0.9677
\]
Problem 4e

What types of numbers $n$ are such that the prob of picking an $(a, b)$ that is cool rel to $n$ is close to 1? Give an example of a number between 1000 and 1200 where the prob is close to 1. What is the prob? Give it to 4 places.

We want $n$ to be PRIME. We take $n = 1001$ which is prime.

The prob of picking a cool pair is

$$\frac{1000 \times 1001}{10001 \times 1001} = \frac{1000}{1001} = 0.999.$$
Problem 4e

What types of numbers $n$ are such that the prob of picking an $(a, b)$ that is cool rel to $n$ is close to 1? Give an example of a number between 1000 and 1200 where the prob is close to 1. What is the prob? Give it to 4 places.

We want $n$ to be PRIME. WE take $n = 1001$ which is prime. The prob of picking a cool pair is

$$\frac{1000 \times 1001}{10001 \times 1001} = \frac{1000}{1001} = 0.999.$$
What types of numbers $n$ are such that the prob of picking an $(a, b)$ that is cool rel to $n$ is far from 1? Give an example of a number between 1000 and 1200 where the prob is far from 1.

A number with LOTS of prime factors. We give two examples but leave it to you to work out the answer $n = 1024 = 2^{10}$.

$n = 4 \times 3 \times 5 \times 17$
What types of numbers $n$ are such that the prob of picking an $(a, b)$ that is cool rel to $n$ is far from 1? Give an example of a number between 1000 and 1200 where the prob is far from 1.

A number with LOTS of prime factors. We give two examples but leave it to you to work out the answer

$n = 1024 = 2^{10}$.
$n = 4 \times 3 \times 5 \times 17$
Problem 5a

List all $a, b$ so that the encode-key and the decode-key for affine are the same. All math is mod 26. Need $(\forall x)[a(ax + b) + b \equiv x]$, so $(\forall x)[a^2x + (ab + b) \equiv 1x + 0]$. We match coefficients
Problem 5a

List all $a, b$ so that the encode-key and the decode-key for affine are the same. All math is mod $26$.

Need $(\forall x)[a(ax + b) + b \equiv x]$, so $(\forall x)[a^2x + (ab + b) \equiv 1x + 0]$. We match coefficients

$$a^2 \equiv 1 \text{ and } ab + b \equiv 0$$
List all $a, b$ so that the encode-key and the decode-key for affine are the same. All math is mod 26.

Need $(\forall x)[a(ax + b) + b \equiv x]$, so $(\forall x)[a^2x + (ab + b) \equiv 1x + 0]$. We match coefficients

$$a^2 \equiv 1 \text{ and } ab + b \equiv 0$$

The first equation yields $a \equiv 1$ or $a \equiv 25$. 

Pairs: $(1, 0), (1, 13), (25, 0), (25, 1), \ldots, (25, 25)$. Note that there are 28 such pairs.
Problem 5a

List all \( a, b \) so that the encode-key and the decode-key for affine are the same. All math is mod 26.
Need \((\forall x)[a(ax + b) + b \equiv x]\), so
\((\forall x)[a^2x + (ab + b) \equiv 1x + 0]\). We match coefficients

\[
a^2 \equiv 1 \quad \text{and} \quad ab + b \equiv 0
\]

The first equation yields \( a \equiv 1 \) or \( a \equiv 25 \).

Case 1 \( a \equiv 1 \), so the \( ab + b \equiv 0 \) is now \( b + b \equiv 0 \), \( b \equiv 0 \) or \( b \equiv 13 \). Pairs: \((1, 0)\), \((1, 13)\).
Problem 5a

List all $a, b$ so that the encode-key and the decode-key for affine are the same. All math is mod 26.

Need $(\forall x)[a(ax + b) + b \equiv x]$, so $(\forall x)[a^2x + (ab + b) \equiv 1x + 0]$. We match coefficients

$$a^2 \equiv 1 \text{ and } ab + b \equiv 0$$

The first equation yields $a \equiv 1$ or $a \equiv 25$.

**Case 1** $a \equiv 1$, so the $ab + b \equiv 0$ is now $b + b \equiv 0$, $b \equiv 0$ or $b \equiv 13$. Pairs: $(1, 0)$, $(1, 13)$.

**Case 2** $a \equiv 25$, so the $ab + b \equiv 0$ is now $25b + b \equiv 0$, so $26b \equiv 0$.

OH, that's ALWAYS TRUE! So ANY $b$ works. Pairs: $(25, b)$ for ANY $0 \leq b \leq 25$. 
Problem 5a

List all $a, b$ so that the encode-key and the decode-key for affine are the same. All math is mod 26. Need $(\forall x)[a(ax + b) + b \equiv x]$, so $(\forall x)[a^2x + (ab + b) \equiv 1x + 0]$. We match coefficients

$$a^2 \equiv 1 \text{ and } ab + b \equiv 0$$

The first equation yields $a \equiv 1$ or $a \equiv 25$.

**Case 1** $a \equiv 1$, so the $ab + b \equiv 0$ is now $b + b \equiv 0$, $b \equiv 0$ or $b \equiv 13$. Pairs: $(1, 0), (1, 13)$.

**Case 2** $a \equiv 25$, so the $ab + b \equiv 0$ is now $25b + b \equiv 0$, so $26b \equiv 0$ OH, thats ALWAYS TRUE! So ANY $b$ works. Pairs: $(25, b)$ for ANY $0 \leq b \leq 25$.

Pairs: $(1, 0) (1, 13), (25, 0), (25, 1), \ldots, (25, 25)$. Note that there are 28 such pairs.
Problem 5b,5c

1) Give a reason why having the encode and decode be the same key is a good idea.
Problem 5b, 5c

1) Give a reason why having the encode and decode be the same key is a good idea. When Alice gives Bob the key, Bob does not have to figure out the inverse. This is not a big deal here, but could be for more complicated ciphers.
1) Give a reason why having the encode and decode be the same key is a good idea.
When Alice gives Bob the key, Bob does not have to figure out the inverse.
This is not a big deal here, but could be for more complicated ciphers.

2) Give a reason why having the encode and decode be the same key is a bad idea.
Problem 5b,5c

1) Give a reason why having the encode and decode be the same key is a good idea. When Alice gives Bob the key, Bob does not have to figure out the inverse. This is not a big deal here, but could be for more complicated ciphers.

2) Give a reason why having the encode and decode be the same key is a bad idea.

If Eve knows Alice and Bob are doing this, the key space goes from 312 to 28. So much easier for Eve to crack the code.