CS70 Midterm 1 Review

Alton Zheng, Edwin Liao, Joy Jeng, Sagar Karandikar, Sung Roa Yoon

Eta Kappa Nu, Mu Chapter
University of California, Berkeley

February 18, 2013

Direct Proof

- Theory:
  - Direct Proof of $P \Rightarrow Q$: Assume P ... Therefore Q
  - This is often useful when you have an easy-to-expand expression as P (For example, in the exercise below)
- Exercise:
  Prove that, if m, n are odd integers, then mn is also an odd integer.
- Solution:

Direct Proof

- Theory:
  - Direct Proof of $P \Rightarrow Q$: Assume P ... Therefore Q
  - This is often useful when you have an easy-to-expand expression as P (For example, in the exercise below)
- Exercise:
  Prove that, if m, n are odd integers, then mn is also an odd integer.
- Solution:

$$\begin{aligned} \text{We can write } m = 2k+1, n = 2q+1 \text{ for some } k, q \in \mathbb{Z} \\ (2k+1)(2q+1) \\ 4kq + 2k + 2q + 1 \\ 2(2kq + k + q) + 1 \\ 2a + 1 \text{ for some } a \in \mathbb{Z} \end{aligned}$$

So mn is, by definition, an odd number

Proof by Contraposition

- Theory:
  - Proof by Contraposition of $P \Rightarrow Q$: Assume $\neg Q$ ... Therefore $\neg P$
    So $\neg Q \Rightarrow \neg P \equiv P \Rightarrow Q$
  - This is often useful when you have an easy-to-expand expression as P (For example, in the exercise below)
- Exercise:
  Prove that, if x^2 is even, then x is even, for all $x \in \mathbb{Z}$
- Solution:

Proof by Contraposition

- Theory:
  - Proof by Contraposition of $P \Rightarrow Q$: Assume $\neg Q$ ... Therefore $\neg P$
    So $\neg Q \Rightarrow \neg P \equiv P \Rightarrow Q$
  - This is often useful when you have an easy-to-expand expression as P (For example, in the exercise below)
- Exercise:
  Prove that, if x^2 is even, then x is even, for all $x \in \mathbb{Z}$
- Solution:

Suppose that x is not even.

Let $x = 2k + 1$ for $k \in \mathbb{Z}$

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

We proved that x^2 is an odd number, so we have completed our proof by contrapositive

Proof by Contradiction

- Theory:
  - Proof by Contradiction of P:
    Assume $\neg P$
    $\ldots$
    R
    $\ldots$
    $\neg R$.
    Contradiction, therefore P
- Exercise:
  Prove that there is no greatest integer.
- Solution:

Proof by Contradiction

- Theory:
  - Proof by Contradiction of P:
    Assume $\neg P$
    ...
    R
    ...
    $\neg R$.
    Contradiction, therefore P
- Exercise:
  Prove that there is no greatest integer.
- Solution: Assume that there is a greatest integer N. But we know that $N+1$ is also an integer (since integers are closed under addition, by definition), and $N+1 > N$ so N is not the greatest integer. Contradiction. Therefore there is no greatest integer.

Proofs by Induction

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Proofs by Induction

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2} = 1$

Proofs by Induction

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2} = 1$

Induction Hypothesis: Assume $P(m)$ for some m.

Proofs by Induction

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2} = 1$

Induction Hypothesis: Assume $P(m)$ for some m.

Induction Step: Prove for $P(m+1)$.

$$\begin{aligned} P(m+1) &= P(m) + (m+1) \\ &= \frac{m(m+1)}{2} + (m+1) \\ &= \frac{m^2 + m + 2(m+1)}{2} \\ &= \frac{m^2 + 3m + 2}{2} \\ &= \frac{(m+1)(m+2)}{2} \end{aligned} \tag{1}$$

Cubed $\rightarrow$ Squared

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i^3 = (\frac{k(k+1)}{2})^2$

Cubed $\rightarrow$ Squared

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i^3 = (\frac{k(k+1)}{2})^2$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i^3 = (\frac{1(1+1)}{2})^2 = 1$

Cubed → Squared

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i^3 = (\frac{k(k+1)}{2})^2$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i^3 = (\frac{1(1+1)}{2})^2 = 1$

Induction Hypothesis: Assume $P(m)$ for some m.

Cubed $\rightarrow$ Squared

Prove by induction $\forall k \in \mathbb{N}, P(k)$, where $\sum_{i=1}^{k} i^3 = (\frac{k(k+1)}{2})^2$

Base Case: $P(1)$. Then $\sum_{i=1}^{1} i^3 = (\frac{1(1+1)}{2})^2 = 1$

Induction Hypothesis: Assume $P(m)$ for some m.

Induction Step: Prove for $P(m+1)$.

$$
\begin{aligned}
P(m+1) &= P(m) + (m+1)^3 \\
&= (\frac{m(m+1)}{2})^2 + (m+1)^3 \\
&= \frac{m^2(m+1)^2}{4} + \frac{4(m+1)(m+1)^2}{4} \\
&= \frac{(m^2+4m+4)(m+1)^2}{4} \\
&= \frac{(m+2)^2(m+1)^2}{4} \\
&= (\frac{(m+1)(m+2)}{2})^2
\end{aligned}
$$

Divisible?

(Fa06 Papadimitriou and Vazirani #2) Prove by induction that for every odd positive integer n, $3^n + 4^n$ is divisible by 7.

Divisible?

(Fa06 Papadimitriou and Vazirani #2) Prove by induction that for every odd positive integer n, $3^n + 4^n$ is divisible by 7.

Base Case: For n $= 1$, we know that $3 + 4 = 7$, which is divisible by 7.

Divisible?

(Fa06 Papadimitriou and Vazirani #2) Prove by induction that for every odd positive integer n, $3^n + 4^n$ is divisible by 7.

Base Case: For n = 1, we know that $3 + 4 = 7$, which is divisible by 7.

Induction Hypothesis: Assume $3^n + 4^n$, where n is some positive odd integer, is divisible by 7.

Divisible?

(Fa06 Papadimitriou and Vazirani #2) Prove by induction that for every odd positive integer n, $3^n + 4^n$ is divisible by 7.

Base Case: For n = 1, we know that $3 + 4 = 7$, which is divisible by 7.

Induction Hypothesis: Assume $3^n + 4^n$, where n is some positive odd integer, is divisible by 7.

Induction Step: We want to prove that $3^{n+2} + 4^{n+2}$ is divisible by 7.

$3^{n+2} + 4^{n+2} = 9 * 3^n + 16 * 4^n$
We know that
$9 * 3^n + 16 * 4^n$ is divisible by 7 if
$9 * 3^n + 16 * 4^n \pmod 7 = 0$.
$9 * 3^n + 16 * 4^n \pmod 7 = 2 * 3^n + 2 * 4^n$
$= 2(3^n + 4^n) \pmod 7$
From the induction hypothesis, we know that $3^n + 4^n$ is divisible by 7, and therefore so is $2(3^n + 4^n)$.

Chocolate

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

Chocolate

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

We will use induction on $r = mn$; induction on the number of pieces in the bar.

Chocolate

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

We will use induction on $r = mn$; induction on the number of pieces in the bar.

Base Case: The minimum number of breaks required is $g(r)$. $r = 1$. $m = 1$, $n = 1$. No breaks are necessary, and we observe that $g(r) = r - 1 = 0$.

Chocolate

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

We will use induction on $r = mn$; induction on the number of pieces in the bar.

Base Case: The minimum number of breaks required is $g(r)$. $r = 1$. $m = 1$, $n = 1$. No breaks are necessary, and we observe that $g(r) = r - 1 = 0$.

Induction Hypothesis: Assume $\forall s \leq k, g(s) = s - 1$. (Strong induction)

Chocolate Step

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

Chocolate Step

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

We will use induction on $r = mn$; induction on the number of pieces in the bar.

Chocolate Step

(Vazirani Fa12 Midterm 1 #3b) You wish to break a standard mn Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

We will use induction on $r = mn$; induction on the number of pieces in the bar.

Induction Step:
Consider $r = k + 1$. Since we have one big piece and $k + 1$ pieces to distribute, we need to begin by making 1 break. This results in two bars, one with $u < k + 1$ and another with $v < k + 1$ pieces, where $u + v = k + 1$. Applying the inductive hypothesis, it takes a minimum of $g(v) = v - 1$ breaks on the bar of size v, and it takes $g(u) = u - 1$ breaks on the bar of size u. The total minimum number of breaks is then $g(k + 1) = 1 + (v - 1) + (u - 1) = (u + v) - 1 = (k + 1) - 1$. Therefore, for any bar of size mn, it takes a minimum of $mn - 1$ breaks.

Stable Marriage Question

Objective: Given that there are n men and n women, match them up (male to female pairing) in such a way that there are no *rogue couples*.

Stable Marriage Question

Objective: Given that there are n men and n women, match them up (male to female pairing) in such a way that there are no *rogue couples*.

Rogue couples: A man and a woman who prefer each other as opposed to their current partners. (BOTH sides must prefer each other to their current partners!)

Few things to note

I'm not going to go over the whole proof with you, for the sake of time, but you should have a look at it again. Instead, how about some pointers to help you remember a few key facts?

Few things to note

I'm not going to go over the whole proof with you, for the sake of time, but you should have a look at it again. Instead, how about some pointers to help you remember a few key facts?

1. **TMA is male-optimal**: You can think of it this way - if all of the males prefer unique woman for their first choice, would the women have ANY say in the matter?
   Remember, male-optimal means that every male has the highest choice woman he can be hoped to paired with in ANY stable pairing.

Few things to note

I'm not going to go over the whole proof with you, for the sake of time, but you should have a look at it again. Instead, how about some pointers to help you remember a few key facts?

1. **TMA is male-optimal**: You can think of it this way - if all of the males prefer unique woman for their first choice, would the women have ANY say in the matter?
   Remember, male-optimal means that every male has the highest choice woman he can be hoped to paired with in ANY stable pairing.
2. **Stable pairing that is both male- and female-optimal**: Is it possible to have both in a stable pairing? Yes. However, that also means that there is only 1 stable pairing possible, as that specific pairing needs to be both Male-optimal AND male-pessimal, female-optimal AND female-pessimal.

Few things to note

I'm not going to go over the whole proof with you, for the sake of time, but you should have a look at it again. Instead, how about some pointers to help you remember a few key facts?

1. **TMA is male-optimal**: You can think of it this way - if all of the males prefer unique woman for their first choice, would the women have ANY say in the matter?
   Remember, male-optimal means that every male has the highest choice woman he can be hoped to paired with in ANY stable pairing.
2. **Stable pairing that is both male- and female-optimal**: Is it possible to have both in a stable pairing? Yes. However, that also means that there is only 1 stable pairing possible, as that specific pairing needs to be both Male-optimal AND male-pessimal, female-optimal AND female-pessimal.
3. **Runtime of TMA**: TMA has runtime of $O(n^2)$. You can think of it this way - even in the worst case situation, there will be at least 1 man who was rejected at each cycle. Since there are n men and each has n choices, there will be at longest n^2 number of iterations.

Applying the logic

Male Pref	1	2	3	4
A	E	F	G	H
B	G	F	E	H
C	E	G	H	F
D	F	E	G	H

If you are told that the male-optimal stable marriage pairing is {(A, E), (B, F), (C, G), (D, H)}, can you have a stable marriage pairing such that D is paired up with someone other than H?

Applying the logic

Male Pref	1	2	3	4
A	E	F	G	H
B	G	F	E	H
C	E	G	H	F
D	F	E	G	H

If you are told that the male-optimal stable marriage pairing is $\{$(A, E), (B, F), (C, G), (D, H)$\}$, can you have a stable marriage pairing such that D is paired up with someone other than H?

No, because if there was such a pairing, then that pairing would have formed a rogue couple in this set.

Go go go!

Now let's try a practice question.
What is the male- and female-optimal pairing in this set?

Male Pref	1	2	3	4
Jim	S	A	M	N
Matt	A	N	M	S
Valerian	N	A	M	S
Tychus	M	N	A	S

Female Pref	1	2	3	4
Sarah	J	M	V	T
Ariel	J	M	V	T
Mira	J	V	M	T
Nova	V	M	J	T

Go go go!

Now let's try a practice question.
What is the male- and female-optimal pairing in this set?

Male Pref	1	2	3	4
Jim	S	A	M	N
Matt	A	N	M	S
Valerian	N	A	M	S
Tychus	M	N	A	S

Female Pref	1	2	3	4
Sarah	J	M	V	T
Ariel	J	M	V	T
Mira	J	V	M	T
Nova	V	M	J	T

The male-optimal pairings are: {(Sarah, Jim), (Ariel, Matt), (Nova, Valerian), (Mira, Tychus)}
The female-optimal pairings are: {(Sarah, Jim), (Ariel, Matt), (Nova, Valerian), (Mira, Tychus)}

Euclid's Extended Algorithm

Evaluate:

$$\text{extended-gcd}(37,10)$$

Show all recursive steps and return values. Use this information to provide a solution, if any to:

$$10x = 1 \bmod 37$$

```
algorithm extended-gcd(x,y):
   if y = 0 then return(x, 1, 0)
   else:
      (d, a, b) := extended-gcd(y, x mod y)
      return((d, b, a - (x div y) * b))
```

Euclid's Extended Algorithm

$$extended - gcd(37, 10) \quad -> \tag{2}$$

$$extended - gcd(10, 7) \quad -> \tag{3}$$

$$extended - gcd(7, 3) \quad -> \tag{4}$$

$$extended - gcd(3, 1) \quad -> \tag{5}$$

$$extended - gcd(1, 0) \quad -> \tag{6}$$

Euclid's Extended Algorithm

$$
\begin{aligned}
extended-gcd(37,10) &\quad -> \qquad && (2)\\
extended-gcd(10,7) &\quad -> \qquad && (3)\\
extended-gcd(7,3) &\quad -> \qquad && (4)\\
extended-gcd(3,1) &\quad -> \qquad && (5)\\
extended-gcd(1,0) &\quad -> \quad returns(1,1,0) && (6)
\end{aligned}
$$

Euclid's Extended Algorithm

$$
\begin{aligned}
extended - gcd(37, 10) &\quad - > && \quad (2)\\
extended - gcd(10, 7) &\quad - > && \quad (3)\\
extended - gcd(7, 3) &\quad - > && \quad (4)\\
extended - gcd(3, 1) &\quad - > \quad returns(1, 0, 1) && \quad (5)\\
extended - gcd(1, 0) &\quad - > \quad returns(1, 1, 0) && \quad (6)
\end{aligned}
$$

Euclid's Extended Algorithm

$$
\begin{aligned}
extended - gcd(37, 10) &\quad -> && (2)\\
extended - gcd(10, 7) &\quad -> && (3)\\
extended - gcd(7, 3) &\quad -> \quad returns(1, 1, -2) && (4)\\
extended - gcd(3, 1) &\quad -> \quad returns(1, 0, 1) && (5)\\
extended - gcd(1, 0) &\quad -> \quad returns(1, 1, 0) && (6)
\end{aligned}
$$

Euclid's Extended Algorithm

$$
\begin{aligned}
extended - gcd(37, 10) &\quad -> && (2)\\
extended - gcd(10, 7) &\quad -> \quad returns(1, -2, 3) && (3)\\
extended - gcd(7, 3) &\quad -> \quad returns(1, 1, -2) && (4)\\
extended - gcd(3, 1) &\quad -> \quad returns(1, 0, 1) && (5)\\
extended - gcd(1, 0) &\quad -> \quad returns(1, 1, 0) && (6)
\end{aligned}
$$

Euclid's Extended Algorithm

$$
\begin{aligned}
extended - gcd(37,10) \quad &-> \quad returns(1,3,-11) && (2)\\
extended - gcd(10,7) \quad &-> \quad returns(1,-2,3) && (3)\\
extended - gcd(7,3) \quad &-> \quad returns(1,1,-2) && (4)\\
extended - gcd(3,1) \quad &-> \quad returns(1,0,1) && (5)\\
extended - gcd(1,0) \quad &-> \quad returns(1,1,0) && (6)
\end{aligned}
$$

Euclid's Extended Algorithm

$$extended - gcd(37, 10) \quad -> \quad returns(1, 3, -11) \tag{2}$$
$$extended - gcd(10, 7) \quad -> \quad returns(1, -2, 3) \tag{3}$$
$$extended - gcd(7, 3) \quad -> \quad returns(1, 1, -2) \tag{4}$$
$$extended - gcd(3, 1) \quad -> \quad returns(1, 0, 1) \tag{5}$$
$$extended - gcd(1, 0) \quad -> \quad returns(1, 1, 0) \tag{6}$$

So a solution for $10x = 1$ mod 37 is $x = -11$, or equivalently, x = 26 mod 37.

Fermat's Little Theorem:

Fermat's Little Theorem:
$a^{p-1} = 1$ mod p (p is a prime)

Calculate 2^{125} mod 127. Hint: 127 is prime.

Fermat's Little Theorem

Calculate 2^{125} mod 127. Hint: 127 is prime.

$$(1)$$
$$(2)$$
$$(3)$$
$$(4)$$
$$(5)$$

Fermat's Little Theorem

Calculate 2^{125} mod 127. Hint: 127 is prime.

$$= \ 2^{-1} \cdot 2^{126} \bmod 127 \tag{1}$$

(2)

(3)

(4)

(5)

Fermat's Little Theorem

Calculate 2^{125} mod 127. Hint: 127 is prime.

$$= 2^{-1} \cdot 2^{126} \bmod 127 \tag{1}$$
$$= 2^{-1} \cdot 1 \bmod 127 \tag{2}$$
$$= 2^{-1} \bmod 127 \text{ (using extended euclid's)} \tag{3}$$
$$\tag{4}$$
$$\tag{5}$$

Fermat's Little Theorem

Calculate 2^{125} mod 127. Hint: 127 is prime.

$$
\begin{aligned}
&= 2^{-1} \cdot 2^{126} \bmod 127 && (1)\\
&= 2^{-1} \cdot 1 \bmod 127 && (2)\\
&= 2^{-1} \bmod 127 \text{ (using extended euclid's)} && (3)\\
&= 64 \bmod 127 && (4)\\
& && (5)
\end{aligned}
$$

Fermat's Little Theorem

Calculate 2^{125} mod 127. Hint: 127 is prime.

$$\begin{aligned}
&= 2^{-1} \cdot 2^{126} \bmod 127 && (1)\\
&= 2^{-1} \cdot 1 \bmod 127 && (2)\\
&= 2^{-1} \bmod 127 \text{ (using extended euclid's)} && (3)\\
&= 64 \bmod 127 && (4)\\
&= 2^{-1} = -63 = 64 \bmod 127 && (5)
\end{aligned}$$

RSA Review

RSA Review

RSA requires:

RSA Review

RSA requires:

- p, q : large prime numbers (approx. 512 bits each, $N = pq$)
- e : positive integer relatively prime to $(p-1)(q-1)$
- d : inverse of $e \pmod{(p-1)(q-1)}$

RSA Review

RSA requires:

- p, q : large prime numbers (approx. 512 bits each, $N = pq$)
- e : positive integer relatively prime to $(p-1)(q-1)$
- d : inverse of $e \pmod{(p-1)(q-1)}$

Public key: (N, e)
Private key: d
Unencrypted message: x
Encrypted message: $x^e \pmod{N}$

RSA Review

RSA requires:

- p, q : large prime numbers (approx. 512 bits each, $N = pq$)
- e : positive integer relatively prime to $(p-1)(q-1)$
- d : inverse of $e \pmod{(p-1)(q-1)}$

Public key: (N, e)
Private key: d
Unencrypted message: $x \; = x^{ed} \pmod{N}$
Encrypted message: $x^e \pmod{N}$

What's wrong with these RSA schemes?

- $p = 3$
- $q = 4$
- $e = 5$
- $d = 5$

1. p, q are too small.
2. ...

What's wrong with these RSA schemes?

- $p = 3$
- $q = 4$
- $e = 5$
- $d = 5$

1. p, q are too small.
2. ... q is not prime!

What's wrong with these RSA schemes?

- $p = 7$
- $q = 11$
- $e = 3$
- $d = 23$

1. p, q are too small.
2. ...
3. ...

What's wrong with these RSA schemes?

- $p = 7$
- $q = 11$
- $e = 3$
- $d = 23$

1. p, q are too small.
2. ... e is not relatively prime to $(p-1)(q-1)$!
3. ...

What's wrong with these RSA schemes?

- $p = 7$
- $q = 11$
- $e = 3$
- $d = 23$

1. p, q are too small.
2. ... e is not relatively prime to $(p-1)(q-1)$!
3. ... therefore, e has no inverse mod $(p-1)(q-1)$ and d does not exist!

What's wrong with these RSA schemes?

- $p = 11$
- $q = 11$
- $e = 9$
- $d = 90$

1. p, q are too small.
2. ...

What's wrong with these RSA schemes?

- $p = 11$
- $q = 11$
- $e = 9$
- $d = 90$

1. p, q are too small.
2. ... d does not equal e^{-1}!

What's wrong with these RSA schemes?

- $p = 11$
- $q = 11$
- $e = 9$
- $d = 90$

1. p, q are too small.
2. ... d does not equal e^{-1}!

So what should d be?

What's wrong with these RSA schemes?

- $p = 11$
- $q = 11$
- $e = 9$
- $d = 90$

1. p, q are too small.
2. ... d does not equal e^{-1}!

So what should d be? $d = 89 : 9 \times 89 \equiv 801 \equiv 1 \pmod{100}$

What's wrong with these RSA schemes?

- $p = 11$
- $q = 11$
- $e = 9$
- $d = 90$

1. p, q are too small.
2. ... d does not equal e^{-1}!

So what should d be? $d = 89 : 9 \times 89 \equiv 801 \equiv 1 \pmod{100}$

(Also, p and q are the same... Semi-related aside: taking the square root of a number does not take a lot of time, so it would not cost much for a hacker to check if $p == q == \sqrt{N}$. It also doesn't take a lot of time for you to generate another large prime - in other words, don't choose $p == q$)

Let's do an example!

Let's do an example!

Start by choosing p, q, e, d.

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$?

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!**

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x\ldots$

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x \ldots$

Well, that's embarrassing. Our encrypted message is the same as our unencrypted message! And everyone will know this because they will have access to our public key (N, e).

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x \ldots$

Well, that's embarrassing. Our encrypted message is the same as our unencrypted message! And everyone will know this because they will have access to our public key (N, e).

Ok, let's use $e = 3$.

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x \ldots$

Well, that's embarrassing. Our encrypted message is the same as our unencrypted message! And everyone will know this because they will have access to our public key (N, e).

Ok, let's use $e = 3$. What should our secret key d be?

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x \ldots$

Well, that's embarrassing. Our encrypted message is the same as our unencrypted message! And everyone will know this because they will have access to our public key (N, e).

Ok, let's use $e = 3$. What should our secret key d be?
$d = 3 : 3^{-1} \equiv 3 \pmod 8$

Let's do an example!

Start by choosing p, q, e, d. Let's use $p = 3, q = 5$.

What are acceptable values for e?
Any number relatively prime to $(p-1)(q-1) = 2 \times 4 = 8$, so $1, 3, 5, 7, 9, \ldots$
(i.e. any odd number)

So let's choose e. How about $e = 1$? **NO!** Why not?

- Unencrypted message $= x$
- Encrypted message $= x^e = x^1 = x \ldots$

Well, that's embarrassing. Our encrypted message is the same as our unencrypted message! And everyone will know this because they will have access to our public key (N, e).

Ok, let's use $e = 3$. What should our secret key d be?
$d = 3 : 3^{-1} \equiv 3 \pmod 8$

Great! Now we're ready to announce our public key (N, e) to the world!

Let's send a message!

We are given $N = 15, e = 3$

Let's send a message!

We are given $N = 15, e = 3$

What are valid messages we can send?

Let's send a message!

We are given $N = 15, e = 3$

What are valid messages we can send?

Any integer in the range [0, 14] because encryption / decryption is done mod N and $N = 15$

Let's send a message!

We are given $N = 15, e = 3$

What are valid messages we can send?
Any integer in the range [0, 14] because encryption / decryption is done mod N and $N = 15$

Why is it a bad idea to send 0 or 1 as our message?

Let's send a message!

We are given $N = 15, e = 3$

What are valid messages we can send?
Any integer in the range [0, 14] because encryption / decryption is done mod N and $N = 15$

Why is it a bad idea to send 0 or 1 as our message?
An adversary can obtain the encrypted message $x^e \pmod{N}$ and knows that the secret message is $x \equiv (x^e)^d \pmod{N}$ for some secret key d. If $x = 0$, then $x^e = 0$ and the adversary can deduce that $x^{ed} = 0$ for any d. There is a similar argument against sending the message $x = 1$.

Let's send a message!

We are given $N = 15, e = 3$

What are valid messages we can send?
Any integer in the range [0, 14] because encryption / decryption is done mod N and $N = 15$

Why is it a bad idea to send 0 or 1 as our message?
An adversary can obtain the encrypted message $x^e \pmod{N}$ and knows that the secret message is $x \equiv (x^e)^d \pmod{N}$ for some secret key d. If $x = 0$, then $x^e = 0$ and the adversary can deduce that $x^{ed} = 0$ for any d. There is a similar argument against sending the message $x = 1$.

From here, we can just choose a message (x), encrypt the message ($x^e \pmod{N}$), and send the message to the person who knows d without having to worry about the message being intercepted. Let's say our message is $x = 2$, which means our encrypted message is $2^3 \pmod{15} = 8$.

Let's decrypt a message!

We receive $x^e = 8$ and we know that $p = 3, q = 5, e = 3, d = 3$

Let's decrypt a message!

We receive $x^e = 8$ and we know that $p = 3, q = 5, e = 3, d = 3$

How do we decrypt this message?

Let's decrypt a message!

We receive $x^e = 8$ and we know that $p = 3, q = 5, e = 3, d = 3$

How do we decrypt this message?
Take x^e and raise it to the d^{th} power mod N:

Let's decrypt a message!

We receive $x^e = 8$ and we know that $p = 3, q = 5, e = 3, d = 3$

How do we decrypt this message?
Take x^e and raise it to the d^{th} power mod N:

$$\begin{aligned}
(x^e)^d \pmod{15} &= 8^3 \pmod{15} \\
&= 512 \pmod{15} \\
&\equiv 2 \pmod{15}
\end{aligned}$$

Let's decrypt a message!

We receive $x^e = 8$ and we know that $p = 3, q = 5, e = 3, d = 3$

How do we decrypt this message?
Take x^e and raise it to the d^{th} power mod N:

$$\begin{aligned}(x^e)^d \pmod{15} &= 8^3 \pmod{15} \\ &= 512 \pmod{15} \\ &\equiv 2 \pmod{15}\end{aligned}$$

Thus, the original message was $x = 2$! We're done! RSA worked!

That's it!

Thanks for coming!
Good luck on your midterm!