COMP 170 – Fall 2008
Midterm 2 Solution

Q1. Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 19$ and sets $n = 11 \cdot 19 = 209$. He then constructs his public key e and private key d and publishes the (n, e) pair.

(a) Bob's private key is $d = 7$.
What is the value of his public key $e?$.

Q1. Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 19$ and sets $n = 11 \cdot 19 = 209$. He then constructs his public key e and private key d and publishes the (n, e) pair.

(a) Bob's private key is $d = 7$.
What is the value of his public key e?.

By the definition of the RSA algorithm $d \cdot e \bmod T = 1$ where

$$T = (p-1)(q-1) = 10 \cdot 18 = 180.$$

Using, e.g., the extended GCD algorithm, we find that the multiplicative inverse of $7 \bmod T$ is $e = 103$.

Q1. Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 19$ and sets $n = 11 \cdot 19 = 209$. He then constructs his public key e and private key d and publishes the (n, e) pair.

(b) Alice wants to send Bob a message M, $0 < M < n$. She calculates $X = M^e \bmod n$ to send Bob and finds that $X = 15$.
What is the value of the original message M?

Q1. Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 19$ and sets $n = 11 \cdot 19 = 209$. He then constructs his public key e and private key d and publishes the (n, e) pair.

(b) Alice wants to send Bob a message M, $0 < M < n$. She calculates $X = M^e \bmod n$ to send Bob and finds that $X = 15$.
What is the value of the original message M?

$$M = X^d \bmod n = 15^7 \bmod 209 = 203.$$

(The last equality can be derived any of multiple ways)

Q2(a) Is $(15^{60} \bmod 61) = (15^{62} \bmod 63)$?

Q2(b) Is $(100^{440} \bmod 89) = (100^{1320} \bmod 89)$?

Q2(c) Evaluate $3^{1052} \bmod 60$.

Q2.(a) Is $\left(15^{60} \bmod 61\right) = \left(15^{62} \bmod 63\right)$?

No.
61 is a prime number so, by Fermat's little theorem,
$15^{60} \bmod 61 = 1.$.

On the other hand, since $3|15$, we also have $3|15^{62}$.

Since $3|63$, this means that $3|(15^{62} \bmod 63),$
so $15^{62} \bmod 63 \neq 1.$

Q2.(b) Is $\left(100^{440} \bmod 89\right) = \left(100^{1320} \bmod 89\right)$?

Yes.
89 is prime so, by Fermat's little theorem,

$$100^{88} \bmod 89 = 1.$$

Since both 440 and 1320 are divisible by 88 we have

$$\left(100^{440} \bmod 89\right) = 1 = \left(100^{1320} \bmod 89\right).$$

Q2.(c) Evaluate $3^{1052} \bmod 60$.

This can be solved by repeated squaring. Set $I_i = 3^{2^i} \bmod 60$. Then

$$
\begin{aligned}
I_0 &= 3 \\
I_1 &= I^0 \cdot I_0 \bmod 60 = 9 \\
I_2 &= I^1 \cdot I_1 \bmod 60 = 21
\end{aligned}
$$

Now notice that $21 \cdot 21 \bmod 60 = 21$ so, for all $i \geq 2$, $I_i = 21$. Since

$$3^{1052} = 3^{1024} \cdot 3^{128}$$

we find

$$(3^{1052} \bmod 60) = (I_7 \cdot I_{10} \bmod 60) = (21^2 \bmod 60) = 21.$$

Q3.

(a) (i) $(p \wedge q) \vee (\neg p \wedge \neg q)$

(ii) $(p \Rightarrow q) \wedge (q \Rightarrow p)$

(b) (i) $\Big(\forall x \in U \;\, p(x)\Big) \;\Rightarrow\; \Big(\forall x \in U \;\, q(x)\Big)$

(ii) $\forall x \in U \; \Big(p(x) \;\Rightarrow\; q(x)\Big)$

(c) (i) $\Big(\forall x \in U \;\, p(x)\Big) \Rightarrow \Big(\exists y \in V \;\, q(y)\Big)$

(ii) $\exists x \in U \; \exists y \in V \; (p(x) \Rightarrow q(y))$

Q3.

(a) (i) $(p \wedge q) \vee (\neg p \wedge \neg q)$

(ii) $(p \Rightarrow q) \wedge (q \Rightarrow p)$

(b) (i) $\Big(\forall x \in U \ p(x)\Big) \ \Rightarrow \ \Big(\forall x \in U \ q(x)\Big)$

(ii) $\forall x \in U \ \Big(p(x) \ \Rightarrow \ q(x)\Big)$

(c) (i) $\Big(\forall x \in U \ p(x)\Big) \Rightarrow \Big(\exists y \in V \ q(y)\Big)$

(ii) $\exists x \in U \ \exists y \in V \ (p(x) \Rightarrow q(y))$

For each pair, either prove that they are logically equivalent or give a counterexample.

Q3.

(a) (i) $(p \wedge q) \vee (\neg p \wedge \neg q)$

(ii) $(p \Rightarrow q) \wedge (q \Rightarrow p)$

Logically equivalent.

Using the fact that $(p \longrightarrow q) \equiv (\neg p \vee q)$ and the distributive laws gives,

$$
\begin{aligned}
(p \Rightarrow q) \wedge (q \Rightarrow p) &= (\neg p \vee q) \wedge (\neg q \vee p) \\
&= (\neg p \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge \neg q) \vee (p \wedge q) \\
&= (p \wedge q) \vee (\neg p \wedge \neg q)
\end{aligned}
$$

Q3.

(b) (i) $\left(\forall x \in U\ p(x)\right) \Rightarrow \left(\forall x \in U\ q(x)\right)$

(ii) $\forall x \in U \left(p(x) \Rightarrow q(x)\right)$

Not logically equivalent.

Let $U = R$, $p(x)$ be $x \geq 0$, and $q(x)$ be $(1-x)^2 \geq (1+x)^2$.

$$\left(\forall x \in R\ x \geq 0\right) \Rightarrow \left(\forall x \in R\ (1-x)^2 \geq (1+x)^2\right)$$

is true because $\left(\forall x \in R\ x \geq 0\right)$ is false.

On the other hand, $\forall x \in R \left(x \geq 0 \Rightarrow (1-x)^2 \geq (1+x)^2\right)$ is false.

Q3.

(c) (i) $$\Big(\forall x \in U\ p(x)\Big) \Rightarrow \Big(\exists y \in V\ q(y)\Big)$$

(ii) $$\exists x \in U\ \exists y \in V\ (p(x) \Rightarrow q(y))$$

Logically equivalent.

Here is the proof in terms of truth values:

$p(x)$	$q(y)$
always true	always false
always true	not always false
not always true	always false
not always true	not always false
$\Big(\forall x\ p(x)\Big) \Rightarrow \Big(\exists y q(y)\Big)$	$\exists x\ \exists y\ (p(x) \Rightarrow q(y))$
false	false
true	true
true	true
true	true

Q3.

(c) (i) $\left(\forall x \in U \ p(x)\right) \Rightarrow \left(\exists y \in V \ q(y)\right)$

(ii) $\exists x \in U \ \exists y \in V \ (p(x) \Rightarrow q(y))$

Logically equivalent.

Alternatively, we can also prove the equivalence using logic laws:

$$\begin{aligned}
\left(\forall x \in U \ p(x)\right) \Rightarrow \left(\exists y \in V \ q(y)\right) \quad &= \quad \neg\left(\forall x \in U \ p(x)\right) \vee \left(\exists y \in V \ q(y)\right) \\
&= \quad \left(\exists x \in U \ \neg p(x)\right) \vee \left(\exists y \in V \ q(y)\right) \\
&= \quad \exists x \in U \ \exists y \in V \ (\neg p(x) \vee q(y)) \\
&= \quad \exists x \in U \ \exists y \in V \ (p(x) \Rightarrow q(y))
\end{aligned}$$

Q4. For each of the three statements below, state whether they are True or False. Justify your answer.

(a): $\forall x \in N \;\; \exists y \in R \;\; \Big(y = 2x + 1\Big)$

(b): $\exists y \in R \;\; \forall x \in N \;\; \Big(y = 2x + 1\Big)$

(c): $\exists p \in Z^{+} \;\; \Big(\forall x \in Z^{+} \;\; \Big[(x < p) \Rightarrow (\exists q \in Z \;\; (x^{p-1} = qp + 1))\Big]\Big)$

Q4.

(a): $\forall x \in N \quad \exists y \in R \quad \Big(y = 2x + 1\Big)$

True. For any $x \in N$, $2x + 1 \in R$

Q4.

(a): $\forall x \in N \;\; \exists y \in R \;\; \left(y = 2x + 1\right)$

True. For any $x \in N$, $2x + 1 \in R$

(b): $\exists y \in R \;\; \forall x \in N \;\; \left(y = 2x + 1\right)$

False. For any $y < 0$, $y = 2x + 1$ cannot be true for any $x \in N$. For any $y \geq 0$, $y = 2x + 1$ is not true for $x = y/2$.

Q4.

(a): $\forall x \in N \ \ \exists y \in R \ \ \Big(y = 2x + 1\Big)$

True. For any $x \in N$, $2x + 1 \in R$

(b): $\exists y \in R \ \ \forall x \in N \ \ \Big(y = 2x + 1\Big)$

False. For any $y < 0$, $y = 2x + 1$ cannot be true for any $x \in N$. For any $y \geq 0$, $y = 2x + 1$ is not true for $x = y/2$.

(c): $\exists p \in Z^+ \ \ \Big(\forall x \in Z^+ \ \ \Big[(x < p) \Rightarrow (\exists q \in Z \ \ (x^{p-1} = qp + 1))\Big]\Big)$

True. According to Fermat's little theorem, the statement is true if we choose p to be a prime number.

Q5. Prove the following statement by contraposition:

If x and y are two integers such that $0 < x \leq y < 34$ and $x \neq y$, then

$$\Big[(x \bmod 5) \neq (y \bmod 5)\Big] \vee \Big((x \bmod 7) \neq (y \bmod 7)\Big].$$

You may not use the Chinese remainder theorem.

Q5. Solution

Let p(n) and q(n) denote the following two sentences:

$$\begin{array}{lcl} p(n) & : & x \text{ and } y \text{ are two integers such that } 0 < x \leq y < 34 \text{ and } x \neq y \\ q(n) & : & \text{either } \ (x \bmod 5) \neq (y \bmod 5) \ \text{ or } \ (x \bmod 7) \neq (y \bmod 7) \end{array}$$

The result that we need to prove can be expressed as the conditional statement $p(n) \Rightarrow q(n)$.

A contrapositive proof corresponds to proving that $\neg q(n) \Rightarrow \neg p(n)$.

Q5. Solution

Let p(n) and q(n) denote the following two sentences:

$p(n)$: x and y are two integers such that $0 < x \leq y < 34$ and $x \neq y$
$q(n)$: either $(x \bmod 5) \neq (y \bmod 5)$ or $(x \bmod 7) \neq (y \bmod 7)$

We first assume that $q(n)$ is false, i.e.,

$$(x \bmod 5) = (y \bmod 5) \text{ and } (x \bmod 7) = (y \bmod 7)$$

This implies $5|x-y$ and $7|x-y$.
Hence, $35|x-y$ and $x = y + 35q$ for some integers, q.
There are three cases to consider:

(i) If $q = 0$, then $x = y$ and $p(n)$ is false.

(ii) If $q < 0$, then $y \geq x + 35$ and $p(n)$ is false.

(iii) If $q > 0$, then $x \geq y + 35$ and $p(n)$ is false.

For all three cases, p(n) is false. Thus we have $\neg q(n) \Rightarrow \neg p(n)$.
By the contrapositive rule of inference, we can conclude that $p(n) \Rightarrow q(n)$.

Q6. Consider the recurrence relation defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 4T(n-1) + 3^n & \text{if } n > 0 \end{cases}$$

Give a closed form solution for $T(n)$.

Q6. By iterating the recurrence we derive that

$$T(n) = 4^n + \sum_{i=1}^{n} 4^{n-i} 3^i. \tag{1}$$

Then,

$$\begin{aligned}
T(n) &= 4^n + \sum_{i=1}^{n} 4^{n-i} 3^i \\
&= 4^n + 4^n \sum_{i=1}^{n} \left(\frac{3}{4}\right)^i \\
&= 4^n + 4^n \frac{3}{4} \sum_{i=0}^{n-1} \left(\frac{3}{4}\right)^i \\
&= 4^n + 3 \cdot 4^n \left(1 - \left(\frac{3}{4}\right)^n\right) \\
&= 4^{n+1} - 3^{n+1}.
\end{aligned}$$

Q7. Consider the recurrence relation defined by

$$T(n) = \begin{cases} 5 & \text{if } n = 1 \\ 9T\left(\frac{n}{3}\right) + 2n & \text{if } n > 1. \end{cases}$$

For the purposes of this problem, you may assume that n is a power of 3.

(a) Give a closed form solution to $T(n)$.

(b) Prove the correctness of your solution using induction.

Q7.

(a)

$$T(n) = 6n^2 - n.$$

(b) Base case:

Let $n = 1$. $T(1) = 5 = 6 \cdot 1^1 - 1$. So the base case is true.

Inductive case:

Suppose the statement is true for 3^{i-1}, with $i > 0$. Let $n = 3^i$.

By definition,

$$\begin{aligned} T\left(\frac{n}{3}\right) &= 9\left(6\left(\frac{n}{3}\right)^2 - \frac{n}{3}\right) + 2n \\ &= 6n^2 - 3n + 2n \\ &= = 6n^2 - n, \end{aligned}$$

so the statement is true for $n = 3^i$.

From the weak principle of mathematical induction, we conclude that the statement is true for $n = 3^i$, $\forall i \geq 0$.

Q8. Prove by induction that if $T(n)$ is defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ \sqrt{1 + 3\sum_{i=0}^{n-1} \left(T(i)\right)^2} & \text{if } n \geq 1. \end{cases}$$

then $\forall n \geq 0$, $T(n) = 2^n$.

Solution:
Base case: Let $n = 0$. $T(0) = 2^0 = 1$. So the base case is true.
Inductive case: Let $n > 0$. The statement is true from 1 to $n - 1$.
i.e.,

$$T(1) = 2^1, \quad T(1) = 2^2, \quad \ldots \quad T(n-1) = 2^{n-1}$$

$$\begin{aligned} T(n) &= \sqrt{1 + 3\sum_{i=0}^{n-1} (T(i))^2} \\ &= \sqrt{1 + 3\sum_{i=0}^{n-1} (2^i)^2} \end{aligned}$$

Solution:

$$
\begin{aligned}
T(n) &= \sqrt{1 + 3\sum_{i=0}^{n-1} 2^{2i}} \\
&= \sqrt{1 + 3\sum_{i=0}^{n-1} 4^{i}} \\
&= \sqrt{1 + 3(\frac{4^n - 1}{4 - 1})} \\
&= \sqrt{1 + 4^n - 1} \\
&= 2^n
\end{aligned}
$$

Based on the strong principle of mathematical induction, we conclude that the statement is true for all integers $\forall n \geq 0$.