Homework 3

10/12

1. For each of the following values of q, generate 5 random members and run the Miller-Rabin test using them. What is the probability that q is prime?

q=10601

Step 1. $q \not\equiv 0(mod 2)$. So q is odd.

Step 2. $(q-1) = 2^k l \Longrightarrow 10600 = 2^3 * 1325$.
k = 3; l = 1325.

Step 3. Choose a random base $a \in \{1, 2, \cdots 10600\}$.

Step 4. Compute the below sequence.
$\{a^l, a^{2l}, a^{4l}, a^{8l}\}$, since k = 3.

Table 1: Test for each random base.

Base	Sequence	Test 1	Test 2
192	2892, 10076, 10600, 1	Prime	Composite
7219	7709, 10076, 10600, 1	Prime	Composit
5435	8244, 525, 10600, 1	Prime	Composite
1169	10076, 10600, 1, 1	Prime	Compoiste
16	1, 1, 1, 1	Prime	Prime

Result. q = 10601 is a Prime and tested as prime by Miller-Rabin with Probability = 1 for the given random bases.

q=101101

Step 1. $q \not\equiv 0(mod 2)$. So q is odd.

Step 2. $(q-1) = 2^k l \Longrightarrow 10600 = 2^2 * 25275$.
k = 2; l = 25275.

Step 3. Choose a random base $a \in \{1, 2, \cdots 101100\}$.

Step 4. Compute the below sequence.
$\{a^l, a^{2l}, a^{4l}\}$, since k = 2.

Table 2: Test for each random base.

Base	Sequence	Test 1	Test 2
21082	39885, 90091, 1	Prime	Composite
101046	42834, 71709, 82720	Composite	Prime
92196	16666, 31109, 31109	Composite	Prime
72167	24452, 90091, 1	Prime	Composite
47752	86659, 1, 1	Prime	Composite

Result. q, $101101 \equiv 0(mod 7)$, is a Composite and tested by Miller-Rabin as prime with Probability = 1 for the given random bases.

q=15841

Step 1. $q \not\equiv 0(mod 2)$. So q is odd.

Step 2. $(q-1) = 2^k l \Longrightarrow 10600 = 2^5 * 495$.
k = 5; l = 495.

Step 3. Choose a random base $a \in \{1, 2, \cdots 15840\}$.

Step 4. Compute the below sequence.
$\{a^l, a^{2l}, a^{4l}, a^{8l}, a^{16l}, a^{32l}\}$, since k = 5.

Table 3: Test for each random base.

Base	Sequence	Test 1	Test 2
14293	6852, 13021, 218, 1, 1, 1	Prime	Composite
15346	1, 1, 1, 1, 1, 1	Prime	Prime
2472	12461, 3039, 218, 1, 1, 1	Prime	Composite
2698	776, 218, 1, 1, 1, 1	Prime	Composite
5057	3380, 3039, 218, 1, 1, 1	Prime	Composite

Result. q, $15841 \equiv 0(mod 7)$, is a Composite and tested by Miller-Rabin as Prime with Probability = 1 for the given random bases.

2. Compute the following

use \bmod like here

1. 7^7 **in** $\mathbb{Z}4$

In $\mathbb{Z}4, [7^7] = 7^7 \bmod 4$
In $\mathbb{Z}4, [7] = [3]$ and $7^3 mod4 = 3$
We can write $7^7 = 7^3 * 7^3 * 7 \implies 7^7 mod4 = (7^3 mod4) * (7^3 mod4) * (7mod4)mod4$
By substitution, we get, $7^7 mod4 = 27mod4 = 3 \ in \ \mathbb{Z}4$

2. 7^{7^7} **in** $\mathbb{Z}4$

In $\mathbb{Z}4, [7^{7^7}] = 7^{7^7} \bmod 4$
From above problem we know, $7^7 = 3$ in $\mathbb{Z}4$
$7^{7^7}\ mod4 = ((7^7 mod4)^7)mod4$
$7^{7^7}\ mod4 = 3^7 mod4 = 3$
$7^{7^7} = 3 \ in \ \mathbb{Z}4$

3. $7^{7^{7^7}}$ **in** $\mathbb{Z}5$

In $\mathbb{Z}5, [7^{7^{7^7}}] = 7^{7^{7^7}} \bmod 5$
5 is a prime number and is a coprime to 7, so by Fermat's little therom, $7^4 mod5 = 1$
Let say $7^{7^7} = r + 4k$, then by applying Fermat's therom, $7^{7^{7^7}} mod5 = (7^r mod5)mod5$
If $7^{7^7} = r + 4k$, then $r = 7^{7^7} mod4$
By above problem, we know that $7^{7^7} mod4 = 3 \implies r = 3$
By substitution, $7^{7^{7^7}}\ mod5 = (7^3 mod5)mod5 = 3mod5$
In $\mathbb{Z}5, 3mod5 = 3 \implies [7^{7^{7^7}}] = 3$ ✓

4/4

3. Compute $2^{3^{4^5}}\ mod\ 79$

79?

79 is a prime number and 2, 7 are coprime. By Fermat's little therom, $2^{78} mod79 = 1$
Let $3^{4^5} = r + 78k$, then, $2^{3^{4^5}}\ mod\ 79 = (2^r)(2^{78})^k mod79$
By applying Fermats therom, $2^{3^{4^5}}\ mod\ 79 = (2^r)mod79$
If $3^{4^5} = r + 78k \implies r = 3^{4^5} mod78$
We can factorize $78 = 2 * 3 * 13$. Now we find modulus of 3^{4^5} for each factor
$3^{4^5} mod2 = 1mod2$
$3^{4^5} mod3 = 0mod3$
For $3^{4^5} mod13$, let $4^5 = x + 12s$, then $3^{4^5} mod13 = (3^4)(3^{12})^s mod13$
13 is a prime and 3, 13 are coprime, by applying Fermats therom,
we can say, $3^{4^5} mod13 = 3mod13$, where x=4
Now we have 3 modulo, $y = 1mod2; y = 0mod3; y = 3mod13$
If we apply chinese remainder therom to solve above modulo, we get $3^{4^5} mod78 = 237mod78$
$\implies r = 237mod78 = 3 \implies 2^{3^{4^5}}\ mod\ 79 = (2^3)mod79$ ✓

Try to clean this up—it's hard to read.

Space out the mod

4/4

4. Prove that if $gcd(m, n) = 1$ *then* $\varphi(m.n) = \varphi(m).\varphi(n)$

Given function $\varphi(n)$ is a set of integers obtained by a modulo (n).
It was given that $gcd(m, n) = 1 \Longrightarrow integer\ m,\ n\ are\ coprime.$

Chinese remainder theorem says that if $q = b_1.b_2$ where b_1, b_2 are positive integers and such that $gcd(b_1, b_2) = 1$, then the below map is isomorphic, that is one-to-one, so, $\lambda_{q,(b_1,b_2)} = \mathbb{Z}/q\mathbb{Z} = (\mathbb{Z}/b_1\mathbb{Z}) \times (\mathbb{Z}/b_2\mathbb{Z})$

If we substitiute $b_1 = m, b_2 = n$ we get below mapping.
$(\mathbb{Z}/mn\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$
$\Longrightarrow \varphi(m.n) = \varphi(m).\varphi(n)$ ✓

parts (ii), (iii)?

2/4