i. Compute the GCD and LCM of $a = 2^{40} \cdot 3^{30}$ and $b = 2^4 \cdot 3^{21} \cdot 5^8$. Leave your answers as prime factorizations.

\[
\begin{align*}
\text{GCD} &= 2^4 \cdot 3^{21} \\
\text{LCM} &= 2^{40} \cdot 3^{30} \cdot 5^8
\end{align*}
\]

ii. Compute the multiplicative order $\nu$ and the inverse of $a = 5 \mod n = 21$ ($\nu$ is smallest s.t. $a^\nu = 1 \mod n$).

\[
\begin{align*}
a \mod n &= 5 \\
a^2 \mod n &= 4 \\
a^3 \mod n &= 20 \\
a^4 \mod n &= 16 \\
a^5 \mod n &= 17 \\
a^6 \mod n &= 1
\end{align*}
\]

$\nu = 6$

\[\text{Inverse} = a^{\nu-1} = a^5 = 17\]

iii. Prove that if two integers satisfy $a + 2b = 81$ their $\gcd(a, b)$ is a power of 3.

\[
\begin{align*}
\gcd(a, b) &| a \\
\gcd(a, b) &| b \\
\Rightarrow \gcd(a, b) &| 2b \\
\gcd(a, b) &| a+2b \\
\Rightarrow \gcd(a, b) &| 81 \\
\Rightarrow \gcd(a, b) &| 3 \cdot 3 \cdot 3 \cdot 3
\end{align*}
\]

For $\gcd(a, b)$ to divide $3^4$, it must be one of $3, 3^2, 3^3, 3^4$ so it must be a power of 3.
iv. Next 3 questions are RSA for \( p = 13, q = 7, e = 29 \). First: compute \( n = pq \) and \( \varphi(n) \)

\[
\begin{align*}
\sqrt{n} &= 91 \\
\varphi(n) &= (13-1)(7-1) \\
&= 12 \cdot 6 \\
\varphi(n) &= 72
\end{align*}
\]

v. Compute the private key \( d \) as inverse of \( e \mod \varphi(n) \) using Extended Euclid Algorithm.

\[
29 \cdot d \mod 72 = 1
\]

\[
\begin{array}{cccccccc}
a & b & q & r & x & y & a \times x + b \times y \\
72 & 29 & 2 & 14 & -2 & 5 & -2(72) + 5(29) = -144 + 145 = 1 \\
29 & 14 & 2 & 1 & 1 & -2 & 29 \cdot 28 = 1 \\
14 & 1 & 14 & 0 & 0 & 1 & \end{array}
\]

\[
d = 5
\]

vi. RSA-Encode \( x = 2 \) using public key \( e = 29 \mod n \). Compute the exponentiation by repeated squaring.

Verify the answer by RSA-Decode it with private key \( d = 5 \) and compare with \( x \). Hand calculators are not allowed, but some calculations are provided (you may need only some of them):

\[
\begin{align*}
74^2 &= 91 \times 60 + 16 \\
256 \times 148 &= 91 \times 416 + 32 \\
32^2 &= 91 \times 11 + 23 \\
23^2 &= 91 \times 5 + 74 \\
74 \times 32 &= 2368 = 91 \times 26 + 2 \rightarrow 74 \times 32 \mod 91 = 2
\end{align*}
\]

\[
x^e = 2^{29} \mod 91
\]

\[
\begin{align*}
\rightarrow 2^{12} \mod 91 &= 1 \\
\rightarrow 2^{12} \cdot 2^{12} \cdot 2^{12} \cdot 2 \mod 91 \\
\rightarrow 1 \cdot 1 \cdot 16 \cdot 2 \mod 91
\end{align*}
\]

\[
x^e = 32
\]

\[
x^{ed} = 32^5 \mod 91
\]

\[
= 32^4 \cdot 32 \mod 91
\]

\[
= 74 \cdot 32 \mod 91
\]

\[
x^{ed} = 2
\]
i. Compute the GCD and LCM of $a = 2^{20} \cdot 3^{20}$ and $b = 2^{6} \cdot 3^{31} \cdot 5^{9}$. Leave your answers as prime factorizations.

\[
\text{gcd}(a, b) = 2^6 \cdot 3^{20}
\]
\[
\text{lcm}(a, b) = 2^{30} \cdot 3^{31} \cdot 5^9
\]

ii. Compute the multiplicative order $v$ and the inverse of $a = 4 \mod n = 21$ ($v$ is smallest s.t. $a^v = 1 \mod n$).

\[
4 \mod 21 = 4
\]
\[
4^2 \mod 21 = 16
\]
\[
4^3 \mod 21 = 1
\]
\[
v = 3
\]
\[
\alpha^{-1} = \alpha^{21-1} \mod n = 4^{21} \mod 21 = 4^2 \mod 21 = 16
\]

iii. Prove that if two integers satisfy $a - 2b = 64$ their gcd$(a, b)$ is a power of 2.

\[
a - 2b = 64 \quad \therefore \quad \gcd(a, b) \text{ is a power of 2}
\]

This occurs since 64 is a power of 2.

The gcd is the smallest exponent of the prime factors shared before $a - 2b$.

b. Since $\gcd(a, b) = \gcd(64, b)$, and 64 only has a prime factor of 2, the gcd must be a power of 2.
iv. Next 3 questions are RSA for $p = 13, q = 7, e = 29$. First: compute $n = pq$ and $\phi(n)$

\[
\begin{align*}
\phi(n) &= (p-1)(q-1) \\
\phi(91) &= 72
\end{align*}
\]

v. Compute the private key $d$ as inverse of $e \mod \phi(n)$ using Extended Euclid Algorithm.

\[
\begin{align*}
\text{gcd}(\phi(n), e) &= \text{gcd}(72, 29) \\
\alpha &= 72 \quad 6 = 29 \quad \alpha_1 = 2 \quad r = 14 \\
\alpha &= 29 \quad 6 = 14 \quad \alpha_1 = 2 \quad r = 1 \\
\alpha &= 14 \quad 6 = 1 \quad \alpha_1 = 4 \quad r = 0
\end{align*}
\]

\[
\begin{align*}
\text{gcd}(72, 29) &= 1
\end{align*}
\]

\[
\begin{align*}
y_{15} &= 5 = \text{inverse of } e \mod \phi(n) = d \\
x &= y_{15} \\
y &= y_{15} \cdot e \quad y = 1 \quad r = 72 \cdot 29 \cdot 5 \cdot 1
\end{align*}
\]

\[
\begin{align*}
x &= 2 \\
y &= 1
\end{align*}
\]

vi. RSA-Encode $x = 2$ using public key $e = 29 \mod n$. Compute the exponentiation by repeated squaring. Verify the answer by RSA-Decode it with private key $d = 5$ and compare with $x$. Hand calculators are not allowed, but some calculations are provided (you may need only some of them):

\[
\begin{align*}
74^2 &= 91 + 60 + 16 \\
256 + 148 &= 91 + 416 + 32 \\
32^3 &= 91 + 11 + 8 \\
23^2 &= 91 + 5 + 74 \\
236 + 2368 &= 91 + 26.0129 \\
64^2 &= 4096 = 91 + 45 + 1 \\
\end{align*}
\]

\[
\begin{align*}
2^{12} &= (2^6)^2 \equiv 2 \\
X &= 29 \quad n = 91 \\
Y &= 2^{29} \mod 91 \\
Y &= 32
\end{align*}
\]

\[
\begin{align*}
\text{Decode } x &= 32 \\
y &= 32 \\
d &= 5 \\
n &= 91
\end{align*}
\]

\[
\begin{align*}
X &= y^d \mod n \\
X &= 32^5 \mod 91 \\
X &= 32 \\
X &= 2
\end{align*}
\]

\[
\begin{align*}
32^4 \mod 91 &= (32^2 \mod 91)^2 \\
32^2 \mod 91 &= 23 \\
23^2 &= 236 + (236 \mod 91) \\
236 = 2366 + (2362 \mod 91) \\
2366 \mod 91 &= 2 \\
32^5 \mod 91 &= (32^4 \mod 91) (32^1 \mod 91) \\
&= (74)(32 \mod 91) \\
&= 2368 \mod 91
\end{align*}
\]
i. Compute the GCD and LCM of \(a = 2^{20} \cdot 3^{40}\) and \(b = 2^9 \cdot 3^{34} \cdot 5^{11}\). Leave your answers as prime factorizations.

\[
\text{GCD} = 2^9 \cdot 3^{41} \\
\text{LCM} = 2^{30} \cdot 3^{40} \cdot 5^{11}
\]

ii. Compute the multiplicative order \(v\) and the inverse of \(a = 8\) mod \(n = 15\) (\(v\) is smallest s.t. \(a^v = 1\) mod \(n\)).

\[
\begin{align*}
10110 & \quad a^1 = 8 \\
10110 & \quad a^2 = 4 \\
10110 & \quad a^3 = 2 \\
10110 & \quad a^4 = 1 \\
\end{align*}
\]

so \(v = 4\), inverse \(= 8^{4-1} = 8^3 = 2\)

iii. Prove that if two integers satisfy \(a - b = 81\) their gcd(a, b) is a power of 3.

\[
10a = 81 + b, \text{ so } \gcd(b, 81 + b) = 3 \text{ what we need.}
\]

Eucld Theorem shows

\[
\gcd(b, 81 + b) = \gcd(6, 81), \text{ and } 81 = 3^4
\]

so 6/3 \(\gcd\) is the shared common prime factors, an
81 only has prime factors that are a power of 3.

The GCD of \(6, 81\) must also only be a power

3.
iv. Next 3 questions are RSA for $p = 13, q = 7, e = 5$. First: compute $n = pq$ and $\varphi(n)$

\[ n = 13 \times 7 = 91 \]
\[ \varphi(n) = (13 - 1)(7 - 1) = 72 \]

v. Compute the private key $d$ as inverse of $e$ mod $\varphi(n)$ using Extended Euclid Algorithm.

\[
\begin{array}{c|cccc}
 a & b & q & r & x & y \\
- & 13 & 72 & 5 & 14 & 2 \\
92 & 5 & 14 & 2 & 29 & -2 \\
52 & 2 & 1 & 20 & 0 & 1 \\
21 & 1 & 2 & 0 & 1 & 1 \\
\end{array}
\]

\[ y_{new} \times prev - y_{new} \times prev \]

\[ \text{verify} \quad 1 - 1 = 1 \]

So, inverse of $e$, ord, $15, 29 \begin{pmatrix} -2.72 + 5.29 \end{pmatrix} = 1$

vi. RSA-Decode $y = 2$ using private key $d = 29$ mod $n$. Compute the exponentiation by repeated squaring.

Verify the answer by RSA-Encode it with public key $e$ and compare with $y$. Hand calculators are not allowed, but some calculations are provided (you may need only some of them):

\[ 74^2 = 91 \times 60 + 16 \]
\[ 256 \times 148 = 91 \times 416 + 32 \]
\[ 32^2 = 91 \times 11 + 23 \]
\[ 23^2 = 91 \times 5 + 74 \]
\[ 74 \times 32 = 2368 = 91 \times 26.0129 \]
\[ 64^2 = 4096 = 91 \times 45 + 1 \]

\[ 2^1 = 2 \quad 2^2 = 4 \quad 2^4 = 16 \quad 2^8 = 256 = 74 \]
\[ 2^{16} = 16 \]
\[ 2^{24} = 1 \quad 2^{24} \cdot 2^5 = 74 \]

\[ 2^{9} = 16 \cdot 74 \cdot 16 = 2 \mod 91 = 2 \times 16 = 32 \]
CS1802 Quiz2 sec16608 Thu13:35 NAME:

i. Compute the GCD and LCM of \( a = 2^{20} \cdot 3^{40} \) and \( b = 2^{8} \cdot 3^{34} \cdot 5^{11} \). Leave your answers as prime factorizations.

\[
gcd(a, b) \text{ is the union of prime factors so } \gcd(a, b) = 2^9 \cdot 3^{14}
\]

\[
lcm(a, b) \text{ is the union of prime factors so } \lcm(a, b) = 2^{10} \cdot 3^{40} \cdot 5^{11}
\]

ii. Compute the multiplicative order \( \nu \) and the inverse of \( a = 8 \mod n = 15 \) (\( \nu \) is smallest s.t. \( a^\nu = 1 \mod n \)).

\[
\gcd(15, 8) = 1 \quad \gcd(8, 7) = 1 \quad \gcd(7, 1) = 1
\]

so \( \gcd(15, 8) = 1 \)

\[
a \cdot b^\nu = \gcd(a, b)
\]

Since \( 2 \cdot 8 = 1 \mod 15 \),

\[
2 \text{ is the inverse of } b \mod 15
\]

iii. Prove that if two integers satisfy \( a - b = 81 \) their \( \gcd(a, b) \) is a power of 3.

\[
\gcd(a, b) = \gcd(b, a - b) = \gcd(b, 81) = \gcd(9, 81) = 9
\]

\[
\gcd(b, 81) \text{ must be a power of } 3 \text{ because } 81 = 3^4, \text{ that is, } 81 \text{ has no prime factors other than } 3. \text{ So } \gcd(a, b) = \gcd(b, a - b) = \gcd(b, 81) \text{ must be a power of } 3.
\]
iv. Next 3 questions are RSA for \( p = 13, q = 7, e = 5 \). First: compute \( n = pq \) and \( \varphi(n) \)

\[
n = 13 \times 7 = 91
\]

\[
\varphi(n) = (p-1)(q-1) = 12 \times 6 = 72
\]

v. Compute the private key \( d \) as inverse of \( e \mod \varphi(n) \) using Extended Euclid Algorithm.

\[
e = 5
\]

\[
ed \equiv 1 \mod \varphi(n)
\]

\[
gcd(72, 5) = 29 - 2 \times 29 - 2 \times 29 = 1
\]

\[
gcd(5, 2) = 1 - 2 = 1
\]

\[
gcd(2, 1) = 0 - 2 = 1
\]

\[
a - 1 \times 72 = 0. \quad y = 1
\]

\[
\text{since } -1 \times 72 + 29 \times 3 = 1
\]

\[
d = 29
\]

vi. RSA-Decode \( y = 2 \) using private key \( d = 29 \mod n \). Compute the exponentiation by repeated squaring.

Verify the answer by RSA-Encode it with public key \( e \) and compare with \( y \). Hand calculators are not allowed, but some calculations are provided (you may need only some of them).

\[
74^2 = 91 \times 60 + 16
\]

\[
256 = 4 \times 64 + 0
\]

\[
256 = 32 \times 8 + 0
\]

\[
256 = 32 \times 8 + 0
\]

\[
2 + 2^2 \times 4 = 16 \times 16 \mod 91
\]

\[
2 \equiv 2 \mod 91
\]

\[
2^{16} \equiv 2 \times 2 \times 2 \mod 91 = 16
\]

\[
2^{16} \mod 91 = 2
\]

\[
\text{decrypted } y = y^d \mod 91
\]

\[
2^{16} \times 2 \mod 91
\]

\[
\text{verify}
\]
i. Compute the GCD and LCM of $a = 2^{20} \cdot 3^{40}$ and $b = 2^{34} \cdot 5^{11}$. Leave your answers as prime factorizations.

$\text{gcd}(a, b) = 2^9 \cdot 3^4$

$\text{lcm}(a, b) = 2^{20} \cdot 3^{40} \cdot 5^{11}$

ii. Compute the multiplicative order $\varphi$ and the inverse of $a = 8 \mod n = 15$ ($\varphi$ is smallest s.t. $a^\varphi = 1 \mod n$).

$p(\varphi) = \{ 0, 8, 8^2 = 64, 8^3 = 512, 8^4 = 131 \}$ so $\varphi = 4$

Inverse of $8 \mod 15 = 8^{4-1} = 8^3 \mod 15 = 2$

$8^2 \mod 15 = 4$

$8^3 \mod 15 = 8 \cdot 4 = 32 \mod 15 = 2$

iii. Prove that if two integers satisfy $a - b = 81$ their $\text{gcd}(a, b)$ is a power of 3.

Since 3 divides 81 where $81 = a - b$, then 3 divides $(a-b)$ if $\text{gcd}(a, b) | a$ and $\text{gcd}(ca, b) | b$, then $\text{gcd}(ca, b) | a-b$

and $a-b$ is a power of 3 so $\text{gcd}(a, b) | a$ power of 3.
iv. Next 3 questions are RSA for $p = 13, q = 7, e = 5$. First: compute $n = pq$ and $\varphi(n)$

$$n = p \cdot q = 13 \cdot 7 = 91$$

$$\varphi(n) = (p-1)(q-1) = (13-1)(7-1) = 12 \cdot 6 = 72$$

v. Compute the private key $d$ as inverse of $e \mod \varphi(n)$ using Extended Euclid Algorithm.

$$d = e^{-1} \mod \varphi(n) = 5^{-1} \mod 72$$

$\gcd(72, 5)$

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$q$</th>
<th>$r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td>5</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

so $\gcd(72, 5) = 1$

$$ax + by = \gcd(a, b)$$

$72(-2) + 5(29) = 1$

so $5^{-1} \mod 72 = 29$

so $d = 29$

vi. RSA-Decode $y = 2$ using private key $d = 29 \mod n$. Compute the exponentiation by repeated squaring. Verify the answer by RSA-Encode it with public key $e$ and compare with $y$. Hand calculators are not allowed, but some calculations are provided (you may need only some of them):

$$74^4 = 91 \cdot 60 + 16$$
$$256 \cdot 148 = 91 \cdot 416 + 32$$
$$32^2 = 91 \cdot 11 + 23$$
$$23^2 = 91 \cdot 5 + 74$$
$$74 \cdot 32 = 2368 = 91 \cdot 26.0129$$
$$64^2 = 4096 = 91 \cdot 45 + 1$$

decode: $x = y^d \mod n = 2^{29} \mod 91 = 2^{(48+4+1)} \mod 91 = 16 \cdot 74 \cdot 16 \cdot 2 \mod 91$

$2^4 \mod 91 = 16$

$2^8 \mod 91 = 74$

$2^{16} \mod 91 = 16$

$2^{24} \mod 91 = 16$

$2^{40} \mod 91 = 16$

encode $y = x^e \mod n = 32^5 \mod 91 = 32^{(141)} \mod 91 = 74 \cdot 32 \mod 91$

$32^2 \mod 91 = 23$

$32^4 \mod 91 = 74$

$91 \cdot 0129 = 1,9929 \div 2$
i. Compute the GCD and LCM of \( a = 2^{40} \cdot 3^{30} \) and \( b = 2^{10} \cdot 3^{5} \cdot 5^{8} \). Leave your answers as prime factorizations.

\[
\text{GCD} = \text{common prime factors} \quad \text{LCM} = a \cdot b / \text{GCD}
\]

\[
\begin{align*}
gcd(a,b) &= 2^{4} \cdot 3^{21} \\
gcd &= \frac{2^{4} \cdot 3^{21} \cdot 5^{8}}{2^{10} \cdot 3^{5} \cdot 5^{8}} \\
lcm(a,b) &= 2^{40} \cdot 3^{30} \cdot 5^{8}
\end{align*}
\]

or

\[
\begin{align*}
a &= 2^{40} \cdot 3^{30} \\
b &= 2^{10} \cdot 3^{5} \cdot 5^{8} \\
gcd &= 2^{4} \cdot 3^{21} \\
lcm &= \frac{2^{40} \cdot 3^{30} \cdot 5^{8}}{2^{10} \cdot 3^{5} \cdot 5^{8}}
\end{align*}
\]

ii. Compute the multiplicative order \( v \) and the inverse of \( a = 7 \mod n = 15 \) (\( v \) is smallest s.t. \( a^{v} = 1 \mod n \)).

\[
P_{a} = \begin{align*}
&7 \mod 15 = 7, \\
&7^{2} \mod 15 = 4, \\
&7^{3} \mod 15 = 13, \\
&7^{4} \mod 15 = 1
\end{align*}
\]

\[
\begin{align*}
v &= 4 \\
a^{v} &= a^{4} = 13
\end{align*}
\]

iii. Prove that if two integers satisfy \( a - b = 64 \) their \( gcd(a,b) \) is a power of 2.

\[
\begin{align*}
gcd(a,b) &= \text{GCD} \\
GCD | a & \Rightarrow GCD | a - b \Rightarrow GCD | 64 \\
\text{Prime factorization of } 64 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{6} \\
GCD | 64 & \Rightarrow GCD | 2^{6} \Rightarrow \text{GCD is a power of two}
\end{align*}
\]

because \( 2^{6} (64) \)'s only unique prime factor is 2, so it is only divisible by the powers of two from 0-6.
iv. Next 3 questions are RSA for \( p = 13, q = 7, e = 5 \). First: compute \( n = pq \) and \( \varphi(n) \)

\[
\begin{align*}
n &= pq = 13 \cdot 7 = 91 \\
\varphi(n) &= (p-1)(q-1) = 12 \cdot 6 = 72
\end{align*}
\]

v. Compute the private key \( d \) as inverse of \( e \mod \varphi(n) \) using Extended Euclid Algorithm.

\[
\begin{align*}
gcd(91, 5) &= 1, e=5 \text{ works} \\
gcd(72, 5) &= 1, \quad d = e^{-1} = b^{-1} \\
\text{ed mod } \varphi(n) &= 1 \\
b^{-1} &= y \mod a = 29
\end{align*}
\]

vi. RSA-Decode \( y = 2 \) using private key \( d = 29 \mod n \). Compute the exponentiation by repeated squaring.

Verify the answer by RSA-Encode it with public key \( e \) and compare with \( y \). Hand calculators are not allowed, but some calculations are provided (you may need only some of them):

\[
\begin{align*}
\begin{array}{c}
74^2 = 91 \times 60 + 16 \\
74 \cdot 148 = 91 \times 416 + 32 \\
32^2 = 91 \times 11 + 23 \\
23^2 = 91 \times 5 + 74 \\
74 \cdot 32 = 2368 = 91 \times 26.0129 \\
64^2 = 4096 = 91 \times 45 + 1
\end{array}
\end{align*}
\]

\[
\begin{align*}
y &= 2 \\
x &= y^d \mod n = 2^{29} \mod 91 \\
x &= 31
\end{align*}
\]