1. Given $A = 6259162$ and $B = 206346$. [15 pts]

   (a) Find the prime factorizations of A and B and use them to find $\gcd(A, B)$.
   Solution:
   We have $A = 2 \cdot 7^2 \cdot 13 \cdot 17^3$ and $B = 2 \cdot 3 \cdot 7 \cdot 17^3$.
   Thus $\gcd(6259162, 206346) = 2 \cdot 7 \cdot 17^3$.

   (b) Find $\gcd(A, B)$ using the Euclidean Algorithm.
   Solution:
   We have:

$$\begin{aligned} 6259162 &= 30(206346) + 68782 \\ 206346 &= 3(68782) + 0 \end{aligned}$$

   Thus $\gcd(6259162, 206346) = 68782$.

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system: [15 pts]

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 5 \bmod 8 \\ x &\equiv 15 \bmod 17 \end{aligned}$$

Solution:
First we solve the three congruences:

- First:

$$\begin{aligned} (8)(17)y_1 &\equiv 1 \bmod 5 \\ 1y_1 &\equiv 1 \bmod 5 \\ y_1 &\equiv 1 \bmod 5 \end{aligned}$$

- Second:

$$\begin{aligned} (5)(17)y_2 &\equiv 1 \bmod 8 \\ 5y_2 &\equiv 1 \bmod 8 \\ y_2 &\equiv 5 \bmod 8 \end{aligned}$$

- Third:

$$\begin{aligned} (5)(8)y_3 &\equiv 1 \bmod 17 \\ 6y_3 &\equiv 1 \bmod 17 \\ y_3 &\equiv 3 \bmod 17 \end{aligned}$$

We then have:

$$x \equiv (2)(8)(17)(1) + (5)(5)(17)(5) + (15)(5)(8)(3) \equiv 4197 \equiv 117 \bmod 680$$

for the smallest, and the second smallest would be 797.

3. For each of $n = 19, 309, 5672, 37699$ find the exact value p_n of the n^{th} prime (however you want) and then approximate value a_n of the n^{th} prime (using the Prime Number Theorem Corollary). Calculate the percentage error [10 pts]

$$\frac{100\,|p_n - a_n|}{p_n}$$

for each.

Solution:
We have:

- For $n = 19$ we have $p_n = 67$ and $a_n = 55.94434060416236$.
  Then the percentage error is:

$$\frac{100|67 - 55.94434060416236|}{67} = 16.500984172891997$$

- For $n = 309$ we have $p_n = 2039$ and $a_n = 1771.6024545614034$.
  Then the percentage error is:

$$\frac{100|2039 - 1771.6024545614034|}{2039} = 13.114151321167071$$

- For $n = 5672$ we have $p_n = 55889$ and $a_n = 49024.78097089825$.
  Then the percentage error is:

$$\frac{100|55889 - 49024.78097089825|}{55889} = 12.281878418117602$$

- For $n = 37699$ we have $p_n = 449929$ and $a_n = 397249.0221764303$.
  Then the percentage error is:

$$\frac{100|449929 - 397249.0221764303|}{449929} = 11.708509081114947$$

4. Find all incongruent solutions mod 124 to the linear system: [10 pts]

$$52x \equiv 4 \bmod 124$$

Solution:
Since $\gcd(52, 124) = 4 \mid 4$ we know there are 4 incongruent solutions. We can simplify the equation by dividing:

$$\begin{aligned} 52x &\equiv 4 \bmod 124 \\ 13x &\equiv 1 \bmod 31 \end{aligned}$$

This has single solution $x_0 \equiv 12 \bmod 31$ Thus a complete set of incongruent solutions is:

$$x \equiv 12, 43, 74, 105 \bmod 124$$

Note: If not trivial, the single solution can be found by first noting the following where the first line comes from finding the gcd as a linear combination of two values, in this case since $\gcd(13, 31) = 1$:

$$\begin{aligned} (12)(13) + (-5)(31) &= 1 \\ (12)(13) + (-5)(31) &= 1 \\ (12)(13) &\equiv 1 \bmod 31 \end{aligned}$$

5. Find all primitive roots for $n = 13$ as follows: First find the smallest positive primitive root. Then use the Theorem from class which yields all the remaining ones. Final answers should be least nonnegative residues. [15 pts]

Solution:

The smallest positive primite root is $r = 2$. We then know that 2^u is a primitive root iff $\gcd(u, \phi(13)) = 1$. Since $\phi(13) = 12$ we need all u with $\gcd(u, 12) = 1$. The u satisfying this are $u = 1, 5, 7, 11$. So we simplify:

$$\begin{aligned} 2^1 &\equiv 2 \bmod 13 \\ 2^5 &\equiv 6 \bmod 13 \\ 2^7 &\equiv 11 \bmod 13 \\ 2^{11} &\equiv 7 \bmod 13 \end{aligned}$$

Thus the primitive roots are 2,6,7,11.

6. It's a fact that $r = 6$ is a primitive root mod 11. [15 pts]

(a) Use this to construct a table of indices for this primitive root.

Solution:

We have the following:

x	1	2	3	4	5	6	7	8	9	10
$\text{ind}_6 x$	0	9	2	8	6	1	3	7	4	5

(b) Use the table of indices to solve the equation: $x^8 \equiv 5 \bmod 11$. Your answer(s) should be mod 11.

Solution:

We have the following:

$$\begin{aligned}
x^8 &\equiv 5 \bmod 11 \\
8\text{ind}_6 x &\equiv \text{ind}_6 5 \bmod \phi(11) \\
8\text{ind}_6 x &\equiv 6 \bmod 10 \\
\text{ind}_6 x &\equiv 2, 7 \bmod 10 \\
x &\equiv 3, 8 \bmod 11
\end{aligned}$$

(c) Use the table of indices to solve the equation: $3^x \equiv 5 \bmod 11$. Your answer(s) should be mod 10.

Solution:

We have the following:

$$\begin{aligned}
3^x &\equiv 5 \bmod 11 \\
x\,\text{ind}_6 3 &\equiv \text{ind}_6 5 \bmod \phi(11) \\
x(2) &\equiv 6 \bmod 10 \\
x &\equiv 3, 8 \bmod 10
\end{aligned}$$

7. Calculate the following Jacobi symbols: [15 pts]

Solution Note: These solution were autogenerated recursively in Python and may take a minute to understand. $R =$ Reduce numerator mod denominator, $QR =$ Quadratic reciprocity, $2 =$ 2-rule.

(a) $\left(\frac{1141}{667}\right)$

Solution:

$\left(\frac{1141}{667}\right) \underset{R}{=} \left(\frac{474}{667}\right)$

We factor the denominator as $667 = 23^1 29^1$:

- ➔ $\left(\frac{474}{23}\right) \underset{R}{=} \left(\frac{14}{23}\right)$

  We factor the numerator as $14 = 2^1 7^1$:

  - ➔ $\left(\frac{2}{23}\right) \underset{2}{=} 1$
  - ➔ $\left(\frac{7}{23}\right) \underset{QR}{=} -\left(\frac{23}{7}\right) \underset{R}{=} -\left(\frac{2}{7}\right) \underset{2}{=} -1$

- ➔ $\left(\frac{474}{29}\right) \underset{R}{=} \left(\frac{10}{29}\right)$

  We factor the numerator as $10 = 2^1 5^1$:

  - ➔ $\left(\frac{2}{29}\right) \underset{2}{=} -1$
  - ➔ $\left(\frac{5}{29}\right) \underset{QR}{=} \left(\frac{29}{5}\right) \underset{R}{=} \left(\frac{4}{5}\right)$

    We factor the numerator as $4 = 2^2$:

    - ➔ $\left(\frac{2}{5}\right)^2 \underset{2}{=} (-1)^2 = 1$

Final answer equals product of ± 1s: 1

(b) $\left(\frac{1141}{51127}\right)$

Solution:

$\left(\frac{85583}{51127}\right) \underset{R}{=} \left(\frac{34456}{51127}\right)$

We factor the denominator as $51127 = 29^1 41^1 43^1$:

- ➔ $\left(\frac{34456}{29}\right) \underset{R}{=} \left(\frac{4}{29}\right)$

  We factor the numerator as $4 = 2^2$:

  - ➔ $\left(\frac{2}{29}\right)^2 \underset{2}{=} (-1)^2 = 1$

- ➔ $\left(\frac{34456}{41}\right) \underset{R}{=} \left(\frac{16}{41}\right)$

  We factor the numerator as $16 = 2^4$:

  - ➔ $\left(\frac{2}{41}\right)^4 \underset{2}{=} 1^4 = 1$

- ➔ $\left(\frac{34456}{43}\right) \underset{R}{=} \left(\frac{13}{43}\right) \underset{QR}{=} \left(\frac{43}{13}\right) \underset{R}{=} \left(\frac{4}{13}\right)$

  We factor the numerator as $4 = 2^2$:

  - ➔ $\left(\frac{2}{13}\right)^2 \underset{2}{=} (-1)^2 = 1$

Final answer equals product of ± 1s: 1

8. Suppose you intercept the following ciphertext from Alice to Bob: [15 pts]

```
2982 2237 3239 11364 8541 7043
```

You know that Bob's public key is $(e, n) = (1655, 11639)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor $n = 11639$, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take.

Solution:
We factor $11639 = (103)(113)$ and so $\phi(11639) = (103 - 1)(113 - 1) = 11424$. We solve $1655d \equiv 1 \bmod 11424$ and get $d \equiv 6599 \bmod 11424$. We use this to decrypt:

$$\begin{aligned}
18^{6599} &\equiv 18 \bmod 11639 \to \texttt{AS} \\
717^{6599} &\equiv 717 \bmod 11639 \to \texttt{HR} \\
2013^{6599} &\equiv 2013 \bmod 11639 \to \texttt{UN} \\
1812^{6599} &\equiv 1812 \bmod 11639 \to \texttt{SM} \\
3^{6599} &\equiv 3 \bmod 11639 \to \texttt{AD} \\
1124^{6599} &\equiv 1124 \bmod 11639 \to \texttt{LY}
\end{aligned}$$

So the plaintext is:

```
ASHRUNSMADLY
```

9. Determine if each of the following sets is well-ordered. If a set is not well-ordered give evidence. If a set is well-ordered no evidence is required. [15 pts]

   (a) $\{0\} \cup \left\{ \frac{n+4}{n} \,\middle|\, n \in \mathbb{Z}^+ \right\}$

   Solution:
   Not well-ordered, the set without 0 has no least element.

   (b) $2\mathbb{Z}$

   Solution:
   Not well-ordered, for example the set itself has no least element.

   (c) $\left\{ \lfloor \sqrt{n} \rfloor \,\middle|\, n \in \mathbb{Z}^+ \right\}$

   Solution:
   Well-ordered.

10. Suppose $p \geq 11$ is an unknown prime. Find all solutions to $x^2 + 8 \equiv 6x \bmod p$. Note that your solutions will be mod p. [15 pts]

Solution:
Observe that for a solution x we would have:

$$\begin{aligned} x^2 + 8 &\equiv 6x \bmod p \\ x^2 - 6x + 8 &\equiv 0 \bmod p \\ (x-2)(x-4) &\equiv 0 \bmod p \end{aligned}$$

Since p is prime we then have either $p \mid (x-2)$ or $p \mid (x-4)$ yielding solutions $x \equiv 2 \bmod p$ and $x \equiv 4 \bmod p$.

11. Consider the inequality: [15 pts]

$$3^n < n!$$

(a) Find the smallest positive integer n_0 for which this is true. Do this however you wish.
Solution:
Testing gives $n_0 = 7$.

(b) Prove by induction that $3^n < n!$ for all $n \geq n_0$.
Solution:
The base case was proven in part (a).
For the inductive step we assume that $3^k < k!$ for $k \geq 7$ and claim that $3^{k+1} < (k+1)!$.
To see this note that:

$$3^{k+1} = (3)3^k < 3k! < (k+1)k! = (k+1)!$$

where the final inequality holds becase $3 < k+1$ because $k \geq 7$.

12. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratic non-residue of p. Prove that $p \equiv \pm 3 \bmod 8$. [15 pts]

Solution:

If a is a QR of p but $2a$ is a QNR of p then $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{2a}{p}\right) = -1$. However $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$ so then $\left(\frac{2}{p}\right) = -1$.

We could only have $p \equiv \pm 3 \bmod 8$ or $p \equiv \pm 1 \bmod 8$.

- If $p \equiv \pm 3 \bmod 8$ then $p = 8k \pm 3$ so then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2 \pm 48k + 9 - 1)/8} = -1$ as desired.
- If $p \equiv \pm 1 \bmod 8$ then $p = 8k \pm 1$ so then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2 \pm 16k + 1 - 1)/8} = 1$.

13. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$. [15 pts]

Solution:

Suppose that $a^n \mid b^n$. Then $ka^n = b^n$ for some $k \in \mathbb{Z}$.

For any prime that appears in the prime factorization of k, that prime must appear with a power which is a multiple of n, since it appears in b^n with a power which is a multiple of n and if it appears in a^n it must also be with a power which is a multiple of n.

But this means $k = p_1^{c_1 n} ... p_m^{c_m n}$ is the prime factorization of k and so $k = (p_1^{c_1} ... p_m^{c_m})^n$ is a perfect square, meaning $\sqrt{k} \in \mathbb{Z}^+$, so that $a\sqrt{k} = b$ and $a \mid b$.

14. Prove that if $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $c \big| (a+b)$ then $\gcd(c, a) = \gcd(c, b) = 1$. [15 pts]

Solution:
We'll show that $\gcd(c, a) = 1$. Suppose $d \mid c$ and $d \mid a$. Since $d \mid c$ and $c \mid (a+b)$ we have $d \mid (a+b)$. This, coupled with the fact that $d \mid a$, implies that $d \mid b$. However $\gcd(a, b) = 1$ and so $d = 1$.

The proof for $\gcd(c, b) = 1$ is identical, mutatis mutandi.