1. Suppose $n$ is a perfect number and $p$ is a prime such that $pn$ is also perfect. Prove $\gcd(p, n) \neq 1$. [5 pts]

**Solution:** Suppose $\gcd(p, n) = 1$. Since $pn$ is perfect we have $\phi(pn) = 2pn$ However since $\phi$ is multiplicative and $n$ is perfect we also have:

\[
\phi(pn) = \phi(p)\phi(n) \\
= (p - 1)2n \\
= 2pn - 2
\]

This is a contradiction.
2. Suppose $p$ and $q$ are distinct odd primes. Prove that there is always some $n$ with $\left(\frac{n}{pq}\right) = -1$. [10 pts]

**Solution:** We know that $\left(\frac{n}{pq}\right) = \left(\frac{n}{p}\right) \left(\frac{n}{q}\right)$ so as long as we can choose $n$ so that one of these is $1$ and the other is $-1$ we are good.

Let $a$ be a quadratic nonresidue mod $p$. We know one exists since there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues mod $p$.

Consider the system:

\[
\begin{align*}
    n &\equiv 1 \pmod{q} \\
    n &\equiv a \pmod{p}
\end{align*}
\]

By the Chinese Remainder Theorem we may solve this. Let $n$ be the solution, then:

\[
\left(\frac{n}{pq}\right) = \left(\frac{n}{p}\right) \left(\frac{n}{q}\right) = \left(\frac{a}{p}\right) \left(\frac{1}{q}\right) = (-1)(1) = -1
\]
3. Suppose \( \text{ord}_p a = 3 \), where \( p \) is an odd prime. Show \( \text{ord}_p (a + 1) = 6 \). [10 pts]

**Solution:** First note that we know \( a^3 \equiv 1 \mod p \) so \( a^3 - 1 \equiv 0 \mod p \). This tells us \( p \mid (a - 1)(a^2 + a + 1) \) so \( p \) divides one of them and since \( a \not\equiv 1 \mod p \) (because \( \text{ord}_p a = 3 \)) we must have \( a^2 + a + 1 \equiv 0 \mod p \).

With this observe that

\[
(a + 1)^6 \equiv (a^2 + 2a + 1)^3 \equiv (a^2 + a + 1 + a)^3 \equiv (0 + a)^3 \equiv a^3 \equiv 1 \mod p
\]

so that the order divides 6.

- If \( \text{ord}_p (a + 1) = 1 \) then \( a + 1 \equiv 1 \mod p \) so \( a \equiv 0 \mod p \) which is not possible because \( \gcd(a, p) \) must be 1.
- If \( \text{ord}_p (a + 1) = 2 \) then \( (a + 1)^2 \equiv 1 \mod p \) so \( a^2 + 2a + 1 \equiv 1 \mod p \) so \( 0 + a \equiv 1 \mod p \) which is not possible since \( \text{ord}_p a = 3 \).
- If \( \text{ord}_p (a + 1) = 3 \) then \( (a + 1)^3 \equiv 1 \mod p \) so \( a^3 + 3a^2 + 3a + 1 \equiv 1 \mod p \) so \( 1 \equiv a^3 + 3(a^2 + a + 1) - 2 \equiv 1 + 3(0) - 2 \equiv -1 \mod p \) so \( p \mid 2 \) which is not possible since \( p \) is an odd prime.

Thus \( \text{ord}_p (a + 1) = 6 \).
4. Use Euler’s theorem to help find the least nonnegative residue of each of the following: [10 pts]

(a) \(14^{1466} \mod 15\)

**Solution:** By Euler’s Theorem since \(\phi(15) = 8\) we have:

\[14^8 \equiv 1 \mod 15\]

Thus it follows that:

\[14^{1466} \equiv 14^{183(8)+2} \equiv 14^2 \equiv 1 \mod 15\]

(b) \(7^{903} \mod 18\)

**Solution:** By Euler’s Theorem since \(\phi(18) = 6\) we have:

\[7^6 \equiv 1 \mod 18\]

Thus it follows that:

\[7^{903} \equiv 7^{150(6)+3} \equiv 7^3 \equiv 1 \mod 18\]
5. Let $p = 19$. For $a = 1, 14, 16$ determine $\text{ord}_p a$ and determine if each $a$ is a primitive root.  

   **Solution:** We know that the order of an element divides $\phi(19) = 18$ so we only need to check $a^k \mod 19$ for $a = 1, 2, 3, 6, 9, 18$. We have:

   $a = 1$: $1^1 \equiv 1$ so $\text{ord}_{14} 1 = 1$

   $a = 14$: $14^1 \equiv 14, 14^2 \equiv 6, 14^3 \equiv 8, 14^6 \equiv 7, 14^9 \equiv 18, 14^{18} \equiv 1$ so $\text{ord}_{14} 14 = 18$

   $a = 16$: $16^1 \equiv 16, 16^2 \equiv 9, 16^3 \equiv 11, 16^6 \equiv 7, 16^9 \equiv 1$ so $\text{ord}_{14} 16 = 9$

   The only one which is a primitive root is 14.
6. It’s a fact that \( r = 8 \) is a primitive root mod 11. 

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

\[ \begin{array}{cccccccccc}
    x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
    \text{ind}_8x & 0 & 7 & 6 & 4 & 8 & 3 & 9 & 1 & 2 & 5 \\
\end{array} \]

Solution: We have the following:

(b) Use the table of indices to solve the equation: \( 3x \equiv 7 \mod 11 \). Your answer(s) should be mod 11.

Solution: We have the following:

\[
3x \equiv 7 \mod 11 \\
\text{ind}_83 + \text{ind}_8x \equiv \text{ind}_87 \mod \phi(11) \\
6 + \text{ind}_8x \equiv 9 \mod 10 \\
\text{ind}_8x \equiv 3 \mod 10 \\
x \equiv 6 \mod 11
\]

(c) Use the table of indices to solve the equation: \( x^2 \equiv 3 \mod 11 \). Your answer(s) should be mod 11.

Solution: We have the following:

\[
x^2 \equiv 3 \mod 11 \\
2\text{ind}_8x \equiv \text{ind}_83 \mod \phi(11) \\
2\text{ind}_8x \equiv 6 \mod 10 \\
\text{ind}_8x \equiv 3, 8 \mod 10 \\
x \equiv 6, 5 \mod 11
\]

(d) Use the table of indices to solve the equation: \( 4x \equiv 3 \mod 11 \). Your answer(s) should be mod 10.

Solution: We have the following:

\[
4^x \equiv 3 \mod 11 \\
x \text{ind}_84 \equiv \text{ind}_83 \mod \phi(11) \\
x(4) \equiv 6 \mod 10 \\
x \equiv 4, 9 \mod 10
\]
7. Find and justify all quadratic residues of the prime $p = 17$. \hspace{1cm} [5 pts]

**Solution:** We calculate:

\[ \begin{align*}
1^2 &\equiv 1 \pmod{17} \\
2^2 &\equiv 4 \pmod{17} \\
3^2 &\equiv 9 \pmod{17} \\
4^2 &\equiv 16 \pmod{17} \\
5^2 &\equiv 8 \pmod{17} \\
6^2 &\equiv 2 \pmod{17} \\
7^2 &\equiv 15 \pmod{17} \\
8^2 &\equiv 13 \pmod{17} \\
9^2 &\equiv 13 \pmod{17} \\
10^2 &\equiv 15 \pmod{17} \\
11^2 &\equiv 2 \pmod{17} \\
12^2 &\equiv 8 \pmod{17} \\
13^2 &\equiv 16 \pmod{17} \\
14^2 &\equiv 9 \pmod{17} \\
15^2 &\equiv 4 \pmod{17} \\
16^2 &\equiv 1 \pmod{17}
\end{align*} \]

So the quadratic residues are: 1, 2, 4, 8, 9, 13, 15, 16
8. Calculate the following Jacobi symbols: [10 pts]

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

(a) \( \left( \frac{1618}{1333} \right) \)

**Solution:**
\[
\left( \frac{1618}{1333} \right) = R \left( \frac{285}{1333} \right)
\]
We factor the denominator as \( 1333 = 31^1 43^1 \):
\[
\Rightarrow \left( \frac{285}{43} \right) = \left( \frac{6}{43} \right)
\]
We factor the numerator as \( 6 = 2^1 3^1 \):
\[
\Rightarrow \left( \frac{6}{43} \right)^2 = 1
\]
\[
\Rightarrow \left( \frac{6}{43} \right) = -\left( \frac{3}{43} \right) = -\left( \frac{1}{3} \right) = -1
\]
\[
\Rightarrow \left( \frac{285}{43} \right) = \left( \frac{27}{43} \right)
\]
We factor the numerator as \( 27 = 3^3 \):
\[
\Rightarrow \left( \frac{3}{43} \right)^3 QR \left( \frac{43}{3} \right)^3 = \left( \frac{-1}{3} \right)^3 = (-1)^3 = -1
\]
Final answer: 1

(b) \( \left( \frac{88588}{47027} \right) \)

**Solution:**
\[
\left( \frac{88588}{47027} \right) = R \left( \frac{41561}{47027} \right)
\]
We factor the denominator as \( 47027 = 31^1 37^1 41^1 \):
\[
\Rightarrow \left( \frac{41561}{31} \right) = \left( \frac{10}{31} \right)
\]
We factor the numerator as \( 21 = 3^1 7^1 \):
\[
\Rightarrow \left( \frac{3}{31} \right) = \left( \frac{7}{31} \right) = -1
\]
\[
\Rightarrow \left( \frac{7}{31} \right) = -\left( \frac{1}{31} \right) = \left( \frac{7}{3} \right) = \left( \frac{1}{3} \right) = 1
\]
\[
\Rightarrow \left( \frac{41561}{31} \right) = \left( \frac{10}{31} \right)
\]
We factor the numerator as \( 10 = 2^1 5^1 \):
\[
\Rightarrow \left( \frac{2}{31} \right) = -1
\]
\[
\Rightarrow \left( \frac{5}{31} \right) = \left( \frac{2}{31} \right) = \left( \frac{2}{5} \right) = -1
\]
\[
\Rightarrow \left( \frac{41561}{41} \right) = \left( \frac{28}{41} \right)
\]
We factor the numerator as \( 28 = 2^2 7^1 \):
\[
\Rightarrow \left( \frac{2}{41} \right)^2 = 1^2 = 1
\]
\[
\Rightarrow \left( \frac{2}{41} \right) = \left( \frac{2}{7} \right) = \left( \frac{2}{7} \right) = \left( \frac{4}{7} \right)
\]
We factor the numerator as \( 6 = 2^1 3^1 \):
\[
\Rightarrow \left( \frac{4}{7} \right) = \left( \frac{6}{7} \right) = \left( \frac{1}{7} \right) = -1
\]
Final answer: 1
9. Suppose Alice wishes to send Bob the sentence: QUINNHOPSMADLY

She knows Bob has RSA encryption key \((e, n) = (1453, 31897)\) so what will the ciphertext be?

**Solution:**

\[
\begin{align*}
QU &\leftrightarrow 1620 \Rightarrow 1620^{1453} \equiv 16134 \mod 31897 \\
IN &\leftrightarrow 813 \Rightarrow 813^{1453} \equiv 30362 \mod 31897 \\
NH &\leftrightarrow 1307 \Rightarrow 1307^{1453} \equiv 30380 \mod 31897 \\
OP &\leftrightarrow 1415 \Rightarrow 1415^{1453} \equiv 27825 \mod 31897 \\
SM &\leftrightarrow 1812 \Rightarrow 1812^{1453} \equiv 506 \mod 31897 \\
AD &\leftrightarrow 3 \Rightarrow 3^{1453} \equiv 30122 \mod 31897 \\
LY &\leftrightarrow 1124 \Rightarrow 1124^{1453} \equiv 5327 \mod 31897
\end{align*}
\]

So the answer is:

\[
16134 \ 30362 \ 30380 \ 27825 \ 506 \ 30122 \ 5327
\]
10. Suppose Bob receives the following message from Alice: [10 pts]

\[
6090 \ 3690 \ 9819 \ 12504 \ 11865 \ 6295 \ 232 \ 6563
\]

If Bob has RSA decryption key \((d, n) = (11653, 13493)\) what will the plaintext be?

**Solution:**

\[
\begin{align*}
6090^{11653} &\equiv 900 \mod 13493 \rightarrow JA \\
3690^{11653} &\equiv 1208 \mod 13493 \rightarrow MI \\
9819^{11653} &\equiv 402 \mod 13493 \rightarrow EC \\
12504^{11653} &\equiv 1708 \mod 13493 \rightarrow RI \\
11865^{11653} &\equiv 418 \mod 13493 \rightarrow ES \\
6295^{11653} &\equiv 1200 \mod 13493 \rightarrow MA \\
232^{11653} &\equiv 311 \mod 13493 \rightarrow DL \\
6563^{11653} &\equiv 2423 \mod 13493 \rightarrow YX
\end{align*}
\]

So the answer is:

JAMIERESMADLY
11. Eve intercepts the following message from Alice to Bob: 

ZJAENXQJEBVWNIV

She knows that this was encrypted using an affine cipher and furthermore she has discovered that the ciphertext letter Q corresponds to the plaintext letter P and the ciphertext letter Z corresponds to the plaintext letter A.

Decrypt the message.

**Solution:** Since Q corresponds to P we have \( C_1 = 16 \) and \( P_1 = 15 \) and so \( 16 \equiv a(15) + b \mod 26 \). and since Z corresponds to A we have \( C_1 = 25 \) and \( P_1 = 0 \). and so \( 25 \equiv a(0) + b \mod 26 \). We then solve the system:

\[
\begin{align*}
    a(0) + b &\equiv 25 \mod 26 \\
    a(15) + b &\equiv 16 \mod 26
\end{align*}
\]

\[
\begin{align*}
    a(-15) &\equiv 9 \mod 26 \\
    a &\equiv 15 \mod 26
\end{align*}
\]

From here we use \( 16 \equiv a(15) + b \mod 26 \) to get \( b \equiv 25 \mod 26 \).

The multiplicative inverse of \( a = 15 \) is \( a^{-1} \equiv 7 \mod 26 \) and so we can decrypt since \( C \equiv 15P + 25 \mod 26 \) implies \( P \equiv 7(C - 25) \mod 26 \).

So we calculate:

\[
\begin{align*}
    Z &\leftrightarrow 25 \Rightarrow P = 7(25 - 25) = 0 \leftrightarrow A \\
    J &\leftrightarrow 9 \Rightarrow P = 7(9 - 25) = 18 \leftrightarrow S \\
    A &\leftrightarrow 0 \Rightarrow P = 7(0 - 25) = 7 \leftrightarrow H \\
    E &\leftrightarrow 4 \Rightarrow P = 7(4 - 25) = 9 \leftrightarrow J \\
    N &\leftrightarrow 13 \Rightarrow P = 7(13 - 25) = 20 \leftrightarrow U \\
    X &\leftrightarrow 23 \Rightarrow P = 7(23 - 25) = 12 \leftrightarrow M \\
    Q &\leftrightarrow 16 \Rightarrow P = 7(16 - 25) = 15 \leftrightarrow P \\
    J &\leftrightarrow 9 \Rightarrow P = 7(9 - 25) = 18 \leftrightarrow S \\
    E &\leftrightarrow 4 \Rightarrow P = 7(4 - 25) = 9 \leftrightarrow J \\
    B &\leftrightarrow 1 \Rightarrow P = 7(1 - 25) = 14 \leftrightarrow O \\
    V &\leftrightarrow 21 \Rightarrow P = 7(21 - 25) = 24 \leftrightarrow Y \\
    W &\leftrightarrow 22 \Rightarrow P = 7(22 - 25) = 5 \leftrightarrow F \\
    N &\leftrightarrow 13 \Rightarrow P = 7(13 - 25) = 20 \leftrightarrow U \\
    I &\leftrightarrow 8 \Rightarrow P = 7(8 - 25) = 11 \leftrightarrow L \\
    I &\leftrightarrow 8 \Rightarrow P = 7(8 - 25) = 11 \leftrightarrow L \\
    V &\leftrightarrow 21 \Rightarrow P = 7(21 - 25) = 24 \leftrightarrow Y
\end{align*}
\]

And so the result is:

ASHJUMPSJOYFULLY