Express \( \text{gcd}(4321, 3456) \) as

\[
\begin{array}{ccc}
4321 & x & y & 4 \\
3456 & 1 & 0 & \text{1} \\
865 & 1 & -1 & \text{1} \\
861 & -3 & 4 & 3 \\
4 & 4 & -5 & \text{1} \\
1 & 262 & 1079 & 215 \\
\end{array}
\]

\[
1 = -863 \times 4321 + 1079 \times 3456
\]
\[ N = 91 = 7 \cdot 13 \]
\[ r = 5 \]
I didn't do 3 since \( \text{gcd}(3, 5 \cdot (12)) \neq 1 \)
\[ S = 5^4 \mod 72 \]

\[
\begin{array}{c|c}
 72 & 0 \\
 50 & 1 \\
 21 & -14 & 14 \\
 1 & -2 & 25 & 2 \\
\end{array}
\]

\[ S = 5^4 \mod 72 = 29. \]

\[ 35^2 \mod 91 = \boxed{42} \]

35 is not relatively prime to 91! 
\[ \text{gcd}(35, 91) = 7 ? \]
(3) How many generators are there in \( \mathbb{Z}/29 \) under addition?

By PR, there are \( \phi(28) \) generators.

\[ \phi(28) = \phi(4) \cdot \phi(7) = 2 \cdot 6 = 12 \]

2 is a generator

\[ 7 \]

28 is already a generator because it is of order 14; so it is of order 28.
(4) Decide whether \( 2435 \) is a QR \( \pmod{2801} \) by checking \( \left( \frac{2435}{2801} \right) \) using Legendre symbols.

\[
\left( \frac{2435}{2801} \right) = \left( \frac{2801}{2435} \right) = \left( \frac{366}{2435} \right) = \left( \frac{2}{2435} \right) \left( \frac{183}{2435} \right)
\]

where \( 2435 \equiv 3 \pmod{8} \)

\[
(-1)(-1) \left( \frac{64135}{183} \right) = (-1)(-1) \left( \frac{56}{183} \right) \equiv (-1)(-1) \left( \frac{8}{183} \right) \left( \frac{7}{183} \right)
\]

\[
\equiv (-1)(-1) \left( \frac{2}{183} \right) \left( \frac{183}{7} \right)
\]

where \( 183 \equiv -1 \pmod{8} \)

\[
= (-1)(-1)(1)(-1)(1) = -1
\]
5) Find \(a, b, \alpha, \beta, r, s\) such that 
\[a^2 + b^2 = 157\]

\[129^2 + 1^2 = (100)(137)\]

\[A = 129, \quad M = 100\]

\[B = 1, \quad \rho = 157\]

\[u = 129 - 100 = 29\]

\[v = 1\]

\[\frac{uA + vB}{m} = 28, \quad \frac{\nuA - uB}{m} = 1\]

Now 
\[28^2 + 1^2 = 5(157)\]

\[A = 28, \quad B = 1, \quad M = 5\]

\[u = 3, \quad v = 1\]

\[\frac{uA + vB}{m} = 19, \quad \frac{\nuA - uB}{m} = 5\]

\[17^2 + 5^2 = 2(157)\]

\[M = 2\]

\[u = 1, \quad v = 1\]

\[\frac{17 + 5}{2} = 11, \quad \frac{17 - 5}{2} = 6\]

\[11^2 + 6^2 = 157\]
(6) Prove that if $2^p - 1$ is prime then

$x = 2^{p-1}(2^p - 1)$ is perfect.

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1}) \sigma(2^p - 1)$$

$2^{p-1}$ and $2^p - 1$ are relatively prime because $2^p - 1$ is as

\begin{align*}
\sigma(x) &= 2^p (2^p - 1) = 2 \sigma(2^{p-1}(2^p - 1)) = 2^p \\
\text{so it is perfect.}
\end{align*}
Show that if \( \gcd(b, m) = 1 \)

and \( \gcd(k, \phi(m)) \neq 1 \)

then \( b \) has one and only one \( k \)-th root \( \text{mod} \ m \) arithmetic

for some \( u \), \( ku + \phi(m)v = 1 \)

\[ b^u \equiv b^u \mod m \]

\[ (b^{-1})^k \equiv b^{ku} \equiv (b^u)^v \equiv b^{kuv} \equiv b^{ku + \phi(m)v} \equiv b^{ku + v} \equiv b^u \]

since \( (\phi(m), v) = 1 \)

\[ b^{\phi(m)v} \equiv 1 \]

so \( b^u \) is a \( k \)-th root.

Now suppose \( x^k \equiv b \mod m \) and \( \gcd(x, m) = 1 \)

then \( x^{ku} \equiv b^u \)

and \( x^{ku} \equiv x^{ku + \phi(m)v} \equiv x \)

so \( x \equiv b^u \), \( x \) is the \( k \)-th root we already know exists.
Pre the Rubin-Miller Theorem.

If $p$ is an odd prime and $0 < a < p$
and $p-1 = 2^k q$, $q$ odd

then either $a^q \equiv 1 \mod p$ or some $2^{i} \equiv -1 \mod p$

where $0 \leq i < k$. You need the FCT and
a fact about roots of polynomials on finite models.

We know that $2^{\frac{p-1}{2}} \equiv 1 \mod p$ by the FLT

so there is a fact $i$ such that $2^i \equiv -1 \mod p$

if $i = 0$ we have $2^0 \equiv 1 \mod p$
otherwise $i = jk$ and we have $(2^{i})^2 \equiv 1 \mod p$

but $2^{i} \not\equiv 1 \mod p$. By Polynomial Roots Theorem
(mom?) $x^2 \equiv 1 \mod p$ has only two roots, -1 and 1.

so $2^{i} \equiv -1 \mod p$

so we have either $a^q \equiv 1 \mod p$ or $a^q \equiv -1$

for some $i$.

$0 \leq i < k$

by contradiction.
9. Suppose there are no Carmichael numbers of the form pq, where p and q are distinct primes.

Suppose n is a Carmichael number and \( n = pq \), p, q odd, \( p \neq q \),

By KC, given we have p - 1 \( \mid (n - 1) \) and q - 1 \( \mid (n - 1) \).

\( n - 1 = pq - 1 \)

We also have p - 1 \( \mid (p - 1)(q - 1) \) and (q - 1) \( \mid (p - 1)(q - 1) \) (common sense).

So p - 1 and q - 1 both go into

\[
\frac{(p - 1)(q - 1) - (pq - 1)}{pq - 1 - p + q - 1} = \frac{pq + p + q - 1 - pq + 1}{p + q - 1} = \frac{p + q - 1}{p + q - 1}
\]

This is impossible for p, q distinct primes, - it must imply

p - 1 \( \mid q - 1 \) and q - 1 \( \mid p - 1 \). So p = q.