Question 1.
Find integers $x$ and $y$ such that
$$314x + 159y = 1.$$\hspace{1cm}

**Solution:** Using the Euclidean algorithm to find the greatest common divisor of $a = 314$ and $b = 159$, we have

$$314 = 1 \cdot 159 + 155$$
$$159 = 1 \cdot 155 + 4$$
$$155 = 38 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

and the last nonzero remainder is $(314, 159) = 1$.

Working from the bottom up, we have

$$1 = 4 - 3$$
$$= 4 - (155 - 38 \cdot 4) = 39 \cdot 4 - 155$$
$$= 39 \cdot (159 - 155) - 155 = 39 \cdot 159 - 40 \cdot 155$$
$$= 39 \cdot 159 - 40(314 - 159) = (-40) \cdot 314 + 79 \cdot 159$$

and therefore,

$$1 = (-40) \cdot 314 + 79 \cdot 159,$$

and one solution is $x = -40, y = 79$.

**Question 2.**
Let $n$ be a composite positive integer and let $p$ be the smallest prime divisor of $n$. Show that if $p > n^{1/3}$, then $n/p$ is prime.

**Solution:** Suppose $p > n^{1/3}$ and that $n/p$ is composite, so that $n = p \cdot a \cdot b$, where $1 < a, b < n$. Let $q$ and $r$ be any prime divisors of $a$ and $b$, respectively, then $q$ and $r$ are also prime divisors of $n$, so that

$$q \geq p \quad \text{and} \quad r \geq p.$$\hspace{1cm}

This implies that

$$p^3 \leq p \cdot q \cdot r \leq p \cdot a \cdot b = n,$$

that is, $p \leq n^{1/3}$, which is a contradiction. Therefore, $n/p$ is prime.
Question 3.

Find all positive solutions in integers to the system of linear equations

\[ x + y + z = 31 \]
\[ 2x + 2y + 3z = 41. \]

Solution: Solving the first equation, we get the two-parameter family of solutions

\[ x = 31 - t, \quad y = t - s, \quad z = s \]

for \( s, t \in \mathbb{Z} \). Since this must also be a solution of the second equation, we must have

\[ 2(31 - t) + 2(t - s) + 3s = 41, \]

that is, \( s = -21 \). Therefore, there are no positive solutions to the given system.

Question 4.

Prove or disprove that if \( a^2 \equiv b^2 \pmod{m} \), then \( a \equiv b \pmod{m} \) or \( a \equiv -b \pmod{m} \).

Solution: The statement is false, as can be seen by taking \( m = 24 \), \( a = 8 \) and \( b = 4 \);

\[ a^2 \equiv 8^2 \equiv 64 \equiv 16 \equiv 4^2 \equiv b^2 \pmod{24}, \]

but \( 8 \not\equiv 4 \pmod{24} \).

Question 5.

Find all positive integers \( m \) such that \( 1066 \equiv 1776 \pmod{m} \).

Solution: We only need find all positive divisors of \( 1776 - 1066 = 710 \), and these are

\[ 1, 2, 5, 10, 71, 142, 355, 710. \]

Question 6.

Show that the difference of two consecutive cubes is never divisible by 5.

Solution: For any integer \( n \), we have

\[ (n + 1)^3 - n^3 = 3n(n + 1) + 1, \]

and it is easily seen that \( n(n + 1) \) is congruent to 0, 1, or 2 modulo 5, so that \( (n + 1)^3 - n^3 \) can only be congruent to 1, 2, or 4 modulo 5.

Question 7.

Find the smallest odd integer \( n \), with \( n > 3 \), such that \( 3 \mid n, 5 \mid n + 2 \), and \( 7 \mid n + 4 \).

Solution: We have to solve the simultaneous congruences

\[ n \equiv 3 \pmod{3} \]
\[ n \equiv 3 \pmod{5} \]
\[ n \equiv 3 \pmod{7} \]

and since 3, 5, and 7 are pairwise relatively prime, their smallest common multiple is \( 3 \cdot 5 \cdot 7 = 105 \), and we may take \( n = 3 + 105 = 108 \).
Question 8.

(a) Find a positive integer $n$ such that $3^2 \mid n$, $4^2 \mid n + 1$, and $5^2 \mid n + 2$.

(b) Can you find a positive integer $n$ such that $2^2 \mid n$, $3^2 \mid n + 1$, and $4^2 \mid n + 2$.

Solution:

(a) We solve the following simultaneous congruences using the Chinese remainder theorem:

\[
\begin{align*}
  n &\equiv 0 \pmod{9} \\
  n &\equiv -1 \equiv 15 \pmod{16} \\
  n &\equiv -2 \equiv 23 \pmod{25}.
\end{align*}
\]

Here

\[
\begin{align*}
  a_1 &= 0, & a_2 &= 15, & a_3 &= 23 \\
  m_1 &= 9, & m_2 &= 16, & m_3 &= 25,
\end{align*}
\]

and

\[
M_1 = 16 \cdot 25 = 400, \quad M_2 = 9 \cdot 25 = 225, \quad M_3 = 9 \cdot 16 = 144.
\]

Also, solving the congruences

\[
\begin{align*}
  M_1 y_1 &\equiv 1 \pmod{m_1} \\
  M_2 y_2 &\equiv 1 \pmod{m_2} \\
  M_3 y_3 &\equiv 1 \pmod{m_3}
\end{align*}
\]

for the inverses $y_1$, $y_2$, and $y_3$, we have

\[
\begin{align*}
  y_1 &\equiv 7 \pmod{9}, & y_2 &\equiv 1 \pmod{16}, & y_3 &\equiv 4 \pmod{25},
\end{align*}
\]

and the unique solution modulo $9 \cdot 16 \cdot 25$ is given by

\[
n = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 15 \cdot 225 \cdot 1 + 23 \cdot 144 \cdot 4 = 3375 + 13248 = 16623.
\]

(b) There does not exist a positive integer $n$ such that

\[
2^2 \mid n, \quad 3^2 \mid n + 1, \quad \text{and} \quad 4^2 \mid n + 2,
\]

since if such an $n$ existed, then we would have

\[
4 \mid n \quad \text{and} \quad 16 \mid n + 2,
\]

however, this implies that $4 \mid n + 2 - n = 2$, which is a contradiction.
Question 9.
What is the last digit of $7^{355}$?

Solution: We have

\[ 7^2 \equiv 9 \pmod{10}, \]
\[ 7^3 \equiv 3 \pmod{10}, \]
\[ 7^4 \equiv 1 \pmod{10}, \]

and $355 = 88 \cdot 4 + 3$, so that

\[ 7^{355} \equiv (7^4)^{88} \cdot 7^3 \equiv 3 \pmod{10}, \]

and the last digit of $7^{355}$ is 3.

Question 10.
What is the remainder when $314^{162}$ is divided by 165?

Solution: We have the following prime power decompositions:

\[ 314 = 157 \cdot 2 \quad \text{and} \quad 165 = 3 \cdot 5 \cdot 11 \]

and the following congruences:

\[ 2^2 \equiv 1 \pmod{3}, \]
\[ 2^4 \equiv 1 \pmod{5}, \]
\[ 2^8 \equiv 1 \pmod{11}, \]

so that $3 \mid 2^8 - 1$, $5 \mid 2^8 - 1$, and $11 \mid 2^8 - 1$, and since the integers 3, 5, and 11 are pairwise relatively prime, then $165 \mid 2^8 - 1$ also, that is,

\[ 2^8 \equiv 1 \pmod{165}. \]

We also have the congruences:

\[ 157 \equiv 1 \pmod{3}, \]
\[ 157^4 \equiv 1 \pmod{5}, \]
\[ 157^5 \equiv 1 \pmod{11}, \]

and again, since $3 \mid 157^{20} - 1$, $5 \mid 157^{20} - 1$, and $11 \mid 157^{20} - 1$, and the integers 3, 5, and 11 are pairwise relatively prime, then $165 \mid 157^{20} - 1$ also, that is,

\[ 157^{20} \equiv 1 \pmod{165}. \]

Therefore, $2^{40} \equiv 1 \pmod{165}$ and $157^{40} \equiv 1 \pmod{165}$, so that $314^{40} \equiv 1 \pmod{165}$, and since $162 = 4 \cdot 40 + 2$, then

\[ 314^{162} \equiv (314^{40})^4 \cdot 314^2 \equiv 314^2 \equiv 91 \pmod{165}. \]
Question 11.
Prove that $a^n - b^n$ is divisible by the prime $n + 1$ if neither $a$ nor $b$ is.

Solution: Note that if $p$ is a prime and $(a,p) = 1$ and $(b,p) = 1$, then from Fermat’s theorem we have

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{and} \quad b^{p-1} \equiv 1 \pmod{p},$$

so that

$$a^{p-1} - b^{p-1} \equiv 0 \pmod{p}.$$

Now, if $n + 1$ a prime and $(a,n+1) = (b,n+1) = 1$, then from the above we have

$$a^n - b^n \equiv 0 \pmod{n+1},$$

that is, $n + 1 | a^n - b^n$.

Question 12.
Suppose that $p$ is an odd prime.

(a) Show that

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

(b) Show that

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

Solution:

(a) Since $p$ is an odd prime and $(k,p) = 1$ for $1 \leq k \leq p - 1$, then Fermat’s theorem implies that

$$k^{p-1} \equiv 1 \pmod{p}$$

for $1 \leq k \leq p - 1$, and therefore

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + 1 + \cdots + 1 \equiv p - 1 \equiv -1 \pmod{p}.$$

(b) Again, from Fermat’s theorem we have

$$k^p \equiv k \pmod{p}$$

for $1 \leq k \leq p - 1$, and therefore

$$1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + p - 1 \equiv p \left( \frac{p-1}{2} \right) \equiv 0 \pmod{p}$$

since $\frac{p-1}{2} \in \mathbb{Z}^+$.

Question 13.
Show that $\sigma(n)$ is odd if $n$ is a power of 2.

Solution: If $n = 2^\alpha$, then

$$\sigma(2^\alpha) = \sum_{d|2^\alpha} d = 1 + 2 + 2^2 + \cdots + 2^\alpha = \frac{2^{\alpha+1} - 1}{2 - 1} = 2^{\alpha+1} - 1,$$

and $\sigma(2^\alpha) = 2^{\alpha+1} - 1$ is odd for all integers $\alpha \geq 0$. 
Question 14.
For which $n$ is $\sigma(n)$ odd?

Solution: We have seen that if $n = 2^\alpha$, then $\sigma(n)$ is odd. Suppose now that $p$ is an odd prime and that $\alpha$ is a positive integer, then

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

and $\sigma(p^\alpha)$ is odd if and only if the sum contains an odd number of terms, that is, if and only if $\alpha$ is an even integer.

Therefore, $\sigma(n)$ is odd if and only if in the prime power decomposition of $n$, every odd prime occurs to an even power, that is, if and only if $n$ is perfect square or $n$ is $2$ times a perfect square.

Question 15.
Find a formula for $\sigma_2(n) = \sum_{d|n} d^2$.

Solution: If $p$ is a prime and $\alpha$ is a positive integer, then

$$\sigma_2(p^\alpha) = \sum_{d|p^\alpha} d^2 = 1 + p^2 + p^4 + \cdots + p^{2\alpha} = \frac{(p^2)^{\alpha+1} - 1}{p^2 - 1} = \frac{p^{2\alpha+2} - 1}{p^2 - 1},$$

and if the prime power decomposition of $n$ is given by

$$n = \prod_{k=1}^r p_k^{\alpha_k},$$

where the $p_k$'s are distinct primes, then

$$\sigma_2(n) = \prod_{k=1}^r \frac{p_k^{2\alpha_k+2} - 1}{p_k^2 - 1}.$$  

Question 16.
It was long thought that even perfect numbers ended alternately in 6 and 8. Show that this is not the case by verifying that the perfect numbers corresponding to the primes

$$2^{13} - 1$$ and $$2^{17} - 1$$

both end in 6.

Solution: Note that $2^4 \equiv 6 \pmod{10}$ and $6^k \equiv 6 \pmod{10}$ for all $k \geq 1$. Now, if $k \equiv 1 \pmod{4}$, then $k = 1 + 4m$ for some integer $m \geq 1$, and

$$2^k \equiv 2^1 \cdot 2^{4m} \equiv 2 \cdot (2^4)^m \equiv 2 \cdot 6^m \equiv 2 \cdot 6 \equiv 2 \pmod{10},$$

so that $2^k - 1 \equiv 1 \pmod{10}$ for all $k \geq 1$, $k \equiv 1 \pmod{4}$.

Also, if $k = 1 + 4m$, then $k - 1 = 4m$ and

$$2^{k-1} \equiv (2^4)^m \equiv 6^m \equiv 6 \pmod{10}$$

for all $k \geq 5$, $k \equiv 1 \pmod{4}$, and therefore

$$2^{k-1} (2^k - 1) \equiv 6 \cdot 1 \equiv 6 \pmod{10}$$

for all $k \geq 5$, $k \equiv 1 \pmod{4}$. The result now follows since both 13 and 17 are congruent to 1 modulo 4.
Question 17.
Show that all even perfect numbers end in 6 or 8.

Solution: We have seen that any even perfect number $n$ has the form

$$n = 2^{k-1} (2^k - 1)$$

where $2^k - 1$ is prime (and hence $k$ is also prime).

If $k \equiv 1 \pmod{4}$, then we saw in the previous problem that the last digit of $n$ is a 6.

Suppose now that $k \equiv 3 \pmod{4}$, then $k = 3 + 4m$ for some integer $m \geq 0$, so that

$$2^k \equiv 2^3 \cdot (2^4)^m \equiv 2^3 \cdot 6^m \equiv 8 \cdot 6 \equiv 8 \pmod{10}$$

and $2^k - 1 \equiv 7 \pmod{10}$.

Also, for all $k \equiv 3 \pmod{4}$:

$$2^{k-1} \equiv 2^2 (2^4)^m \equiv 4 \cdot 6 \equiv 4 \pmod{10},$$

so that

$$n = 2^{k-1} (2^k - 1) \equiv 4 \cdot 7 \equiv 8 \pmod{10}$$

for all $k \equiv 3 \pmod{4}$.

Question 18.
If $n$ is an even perfect number, with $n > 6$, show that the sum of its digits is congruent to 1 modulo 9.

Solution: Since $10^k \equiv 1 \pmod{9}$ for all $k \geq 0$, then any positive integer $n$ is congruent modulo 9 to the sum of its digits, so we only need to show that if

$$n = 2^{k-1} (2^k - 1), \; k \geq 3$$

is an even perfect number, then $n$ is congruent to 1 modulo 9.

Let $n = 2^{k-1} (2^k - 1)$ be an even perfect number, $n > 6$, then $2^k - 1$ and $k$ are both odd primes. Note that

$$2^2 \equiv 4 \pmod{9}, \; \quad 2^3 \equiv 8 \equiv -1 \pmod{9}, \; \quad 2^6 \equiv 1 \pmod{9}.$$ 

Also, since $k$ is prime, then $k \equiv \pm 1 \pmod{6}$.

If $k \equiv 1 \pmod{6}$, then $k = 1 + 6m$ for some $m \geq 1$, so that

$$2^k \equiv 2 \cdot (2^6)^m \equiv 2 \pmod{9},$$

and

$$2^k - 1 \equiv 2 - 1 \equiv 1 \pmod{9}.$$

Also,

$$2^{k-1} \equiv (2^6)^m \equiv 1 \pmod{9},$$

so that

$$n = 2^{k-1} (2^k - 1) \equiv 1 \pmod{9}$$

if $k \equiv 1 \pmod{6}$.
If \( k \equiv 1 \pmod{6} \), then \( k = 5 + 6m \) for some \( m \geq 0 \), so that
\[
2^k \equiv 2^5 \cdot (2^6)^m \equiv 5 \pmod{9},
\]
and
\[
2^k - 1 \equiv 5 - 1 \equiv 4 \pmod{9}.
\]
Also,
\[
2^{k-1} \equiv 2^4 \cdot (2^6)^m \equiv 7 \pmod{9},
\]
so that
\[
n = 2^{k-1} (2^k - 1) \equiv 4 \cdot 7 \equiv 28 \equiv 1 \pmod{9}
\]
if \( k \equiv 1 \pmod{6} \).

**Question 19.**
Show that if \( n \) is odd, then \( \phi(4n) = 2\phi(n) \).
**Solution:** If \( n \) is odd, then \( (4, n) = 1 \), so that
\[
\phi(4n) = \phi(4) \cdot \phi(n) = 2\phi(n).
\]

**Question 20.**
Perfect numbers satisfy \( \sigma(n) = 2n \). Which \( n \) satisfy \( \phi(n) = 2n \)?
**Solution:** If \( n \) is a positive integer and \( \phi(n) = 2n \), then since
\[
\phi(n) \leq n - 1,
\]
this implies that \( 2n \leq n - 1 \), that is, \( n \leq -1 \), which is a contradiction. Therefore, there are no positive integers \( n \) for which \( \phi(n) = 2n \).

**Question 21.**
Note that
\[
1 + 2 = \frac{3}{2} \cdot \phi(3)
\]
\[
1 + 3 = \frac{4}{2} \cdot \phi(4)
\]
\[
1 + 2 + 3 + 4 = \frac{5}{2} \cdot \phi(5)
\]
\[
1 + 5 = \frac{6}{2} \cdot \phi(6)
\]
\[
1 + 2 + 3 + 4 + 5 + 6 = \frac{7}{2} \cdot \phi(7)
\]
\[
1 + 3 + 5 + 7 = \frac{8}{2} \cdot \phi(8)
\]
Guess a theorem!
**Solution:** The theorem was one that we proved in class, namely,
\[
\sum_{\substack{k=1 \\
(k,n)=1}}^{n} k = \frac{n}{2} \cdot \phi(n).
\]
Question 22.
Find all solutions of \( \phi(n) = 4 \), and prove that there are no more.

**Solution:** If the prime power decomposition of the positive integer \( n \) is given by

\[
n = 2^\alpha \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},
\]

where the \( p_i \)'s are distinct odd primes, then

\[
\phi(n) = 2^{\alpha - 1} \cdot p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1),
\]

and it is clear that if \( \phi(n) = 4 \) then \( n \) can have no more than 2 odd prime factors and these must occur to the first power. It is also clear that the exponent of the power of 2 must be less than or equal to 3.

Thus, if \( \phi(n) = 4 \), then \( n \) must have one of the forms

\[
\begin{align*}
n &= 2^\alpha & \text{for } \alpha \leq 3, \\
n &= 2^\alpha \cdot p & \text{for } \alpha \leq 2, \ p \ \text{an odd prime} \\
n &= 2^\alpha \cdot p \cdot q & \text{for } \alpha \leq 1, \ p, \ q \ \text{odd primes}
\end{align*}
\]

In the first case, if \( n = 2^\alpha \), then \( \phi(n) = 2^{\alpha - 1} = 4 \) if and only if \( \alpha - 1 = 2 \), that is, \( \alpha = 3 \), so \( n = 8 \) is one solution to \( \phi(n) = 4 \).

In the second case, if \( n = 2^\alpha \cdot p \), where \( p \) is an odd prime, then \( \phi(n) = 2^{\alpha - 1}(p - 1) \), and \( \phi(n) = 4 \) if and only if either \( \alpha - 1 = 1 \) and \( p - 1 = 2 \), or \( \alpha - 1 = 0 \) and \( p - 1 = 4 \), or \( \alpha = 0 \) and \( p - 1 = 4 \). Thus, \( n \) is a solution to \( \phi(n) = 4 \) if and only if \( n = 2 \cdot 3 = 6 \) or \( n = 2 \cdot 5 = 10 \), or \( n = 1 \cdot 5 = 5 \).

In the third case, if \( n = 2^\alpha \cdot p \cdot q \), where \( p \) and \( q \) are distinct odd primes, then \( \phi(n) = 2^{\alpha - 1}(p - 1)(q - 1) \), and since both \( p - 1 \) and \( q - 1 \) are even, then we must have \( \alpha = 0 \). Also, since \( p \) and \( q \) are distinct odd primes, then \( (p - 1)(q - 1) = 4 \) implies that one of \( p - 1 \) or \( q - 1 \) equals 1 and the other equals 4, which is a contradiction. Thus, in this case \( \phi(n) \neq 4 \), and there are no solutions.

Therefore, the only solutions to \( \phi(n) = 4 \) are 5, 8, 10, and 12.

**Question 23.**
Show that if \( (m, n) = 2 \), then \( \phi(m \cdot n) = 2 \cdot \phi(m) \cdot \phi(n) \).

**Solution:** Let \( m = 2^r \cdot M \) and \( n = 2^s \cdot N \) where \( M \) and \( N \) are odd and one of \( r \) or \( s \) is 1, then \( (M, N) = 1 \) so that

\[
\phi(m \cdot n) = 2^{r+s-1} \cdot \phi(M) \cdot \phi(N),
\]

and

\[
\phi(m) \cdot \phi(n) = 2^{r-1} \cdot \phi(M) \cdot 2^{s-1} \cdot \phi(N) = 2^{r+s-2} \cdot \phi(M) \cdot \phi(N),
\]

and therefore

\[
2 \cdot \phi(m) \cdot \phi(n) = 2^{r+s-1} \cdot \phi(M) \cdot \phi(N) = \phi(m \cdot n).
\]
Question 24.
Show that if $n - 1$ and $n + 1$ are both primes, with $n > 4$, then $\phi(n) \leq \frac{n}{3}$.

**Solution:** Since $n > 4$, then $n - 1 > 3$, and since one of the consecutive integers $n - 1$, $n$, and $n + 1$ is divisible by 3 and $n - 1$ and $n + 1$ are primes greater than 3, then $3 \mid n$. Also, $n$ must be even, since $n - 1$ and $n + 1$ are odd primes, so that $2 \mid n$.

Since $(2,3) = 1$, and $n$ is a common multiple of 2 and 3, then $6 = 2 \cdot 3 = [2,3]$ also divides $n$, and we can write

$$n = 2^a \cdot 3^b \cdot N$$

where $a \geq 1$ and $b \geq 1$, and $(2,N) = (3,N) = 1$.

Therefore,

$$\phi(n) = 2^a \cdot 3^{b-1} \cdot \phi(N) \leq 2^a \cdot 3^{b-1} \cdot N = \frac{n}{3}.$$  

Question 25.
One of the primitive roots of 19 is 2. Find all of the others.

**Solution:** Since $(19) = 18$, and $(18) = 6$, then there are 6 incongruent primitive roots of 19, and they are

$$2^u, 1 \leq u \leq 18, \text{ with } (u, 18) = 1,$$

that is, the incongruent primitive roots of 19 are 2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}.

Question 26.
Suppose that $p$ is a prime and $a$ has order 4 modulo $p$. What is the least positive residue of $(a + 1)^4$ modulo $p$?

**Solution:** Since $a^4 \equiv 1 \pmod{p}$, then $p \geq 5$, and since

$$p \mid a^4 - 1 = (a^2 - 1)(a^2 + 1),$$

and $p$ is prime with $a^2 \not\equiv 1 \pmod{p}$, then $p \mid a^2 + 1$, that is, $a^2 \equiv -1 \pmod{p}$.

Therefore,

$$(a + 1)^4 \equiv a^4 + 4a^3 + 6a^2 + 4a + 1 \equiv 1 - 4a - 6 + 4a + 1 \equiv 2 - 6 \equiv -4 \equiv p - 4 \pmod{p},$$

and $(a + 1)^4 \equiv (p - 4) \pmod{p}$, so the least positive residue of $(a + 1)^4$ modulo $p$ is $p - 4$.

Question 27.
If $r$ is a primitive root of the prime $p$, show that two consecutive powers of $r$ have consecutive least positive residues modulo $p$, that is, show that there exists an integer $k \geq 1$ such that

$$r^{k+1} \equiv r^k + 1 \pmod{p}.$$ 

**Solution:** The set

$$\{1, r, r^2, \ldots, r^{p-1}\}$$

forms reduced residue system modulo $p$. Therefore, since the $\phi(p) = p - 1$ integers

$$\{r^2 - r, r^3 - r^2, r^4 - r^3, \ldots, r^{p-1} - r^{p-2}\}$$

are all incongruent modulo $p$, they also form a reduced residue system modulo $p$, and there must be an integer $k$, with $1 \leq k \leq p - 1$, such that

$$r^{k+1} - r^k \equiv 1 \pmod{p}.$$
Question 28.

Show that if $p$ is an odd prime and $a$ is a quadratic residue modulo $p$, and $a \cdot b \equiv 1 \pmod{p}$, then $b$ is also a quadratic residue modulo $p$.

SOLUTION: There exists an integer $x$ such that $x^2 \equiv a \pmod{p}$, so that

$$(x \cdot b)^2 \equiv x^2 \cdot b^2 \equiv a \cdot b^2 \equiv (a \cdot b) \cdot b \equiv 1 \cdot b \equiv b \pmod{p},$$

and $b$ is also a quadratic residue modulo $p$. 