Solutions to selected homework problems. Sections 4.2-4.3

4.2.44. Let \( n \) denote how many cents each child was given. Then \( n \equiv 13 \equiv 3 \pmod{5} \), \( n \equiv 3 \pmod{6} \), \( n \equiv 2 \pmod{11} \), and \( 300 \leq n < 600 \). We can look for a solution in the form \( n = 5 \cdot 6 \cdot x + 5 \cdot 11 \cdot y + 6 \cdot 11 \cdot z \). Then we get \( z \equiv 3 \pmod{5} \), \( y \equiv 5 \cdot 11 \cdot y \equiv 3 \pmod{6} \), \( 5 \cdot 6 \cdot x \equiv 2 \pmod{11} \), i.e., \(-3x \equiv 2 \pmod{11} \). The last congruence has a solution \( x \equiv 3 \pmod{11} \). Thus,

\[
 n \equiv 5 \cdot 6 \cdot 3 + 5 \cdot 11 \cdot 3 + 6 \cdot 11 \cdot 3 \equiv 453 \pmod{5 \cdot 6 \cdot 11}
\]

The inequalities on \( n \) imply that \( n = 453 \).

4.2.51. First, pick \( k \) distinct primes \( p_1, \ldots, p_k \). Then apply the Chinese theorem to find \( n \) such that \( n \equiv -1 \pmod{p_1^2} \), \( n \equiv -2 \pmod{p_2^2} \), \ldots, \( n \equiv -k \pmod{p_k^2} \). Then each of the numbers \( n+1, n+2, \ldots, n+k \) will not be square free (since \( n+i \) is divisible by \( p_i^2 \)).

4.3.16. Since \( \phi(25) = 20 \) we have

\[
 9^{13} \equiv 9^{3} \equiv 27^2 \equiv 2^2 \equiv 4 \pmod{25}.
\]

4.3.24. 20! is divisible by 3 and by 7, hence, it is divisible by 21, since 3 and 7 are relatively prime.

4.3.34. Let \( n \) be the order of \( a \) modulo \( b \). Then \( a^n \equiv 1 \pmod{b} \). Hence,

\[
 c^n \equiv (a^k)^n \equiv (a^n)^k \equiv 1 \pmod{b}.
\]

Hence, the order of \( c \) modulo \( b \) does not exceed \( n \).

4.3.39. For \( x = ca^{\phi(b)-1} \) we have

\[
 ax \equiv ca^{\phi(b)} \equiv c \pmod{b}
\]

by Euler’s theorem.

4.3.49. Let us denote \( d = (j, p-1) \), \( n = (p-1)/d \). We claim that for an integer \( m \) one has \( (p-1)|mj \) if and only if \( n|m \). Indeed, \( (p-1)|mj \) if and only if \( \frac{p-1}{d}|m\frac{j}{d} \), which is equivalent to \( \frac{p-1}{d}|m \) (since \( (\frac{p-1}{d}, \frac{j}{d}) = 1 \)).

Now recall that \( a^{mj} \equiv 1 \pmod{p} \) if and only if \( mj \) is divisible by the order of \( a \) (Theorem 4.6). Thus, \( a^{mj} \equiv 1 \pmod{p} \) if and only if \( (p-1)|mj \), i.e., \( n|m \). Thus, \( n \) is the smallest number such that \( (a^j)^n \equiv 1 \pmod{p} \), so by definition, \( n \) is the order of \( a^j \).