Math 211

Assignment 6 - Solutions

1. Let \( x \) denote the number of coins in the chest. We then have the following conditions:

\[
\begin{align*}
x & \equiv 3 \pmod{17} \\
x & \equiv 4 \pmod{11} \\
x & \equiv 0 \pmod{7}.
\end{align*}
\]

Since \( \gcd(17, 16) = \gcd(17, 11) = \gcd(17, 7) = \gcd(16, 11) = \gcd(16, 7) = \gcd(11, 7) = 1 \), we can apply the formula of the Chinese Remainder Theorem. Here \( m = 17 \cdot 16 \cdot 11 \cdot 7 = 20944 \), and

\[
\begin{align*}
m'_1 &= 17 \cdot 16 \cdot 11 \cdot 7 \\
m'_2 &= 17 \cdot 16 \cdot 11 \cdot 7 \\
m'_3 &= 17 \cdot 16 \cdot 11 \cdot 7 \\
m'_4 &= 17 \cdot 16 \cdot 11 \cdot 7
\end{align*}
\]

Thus, since here \( a_1 = 3, a_2 = 10, a_3 = 4, a_4 = 0 \), we get

\[
x \equiv a_1 m'_1 + a_2 m'_2 + a_3 m'_3 + a_4 m'_4 \pmod{m} \equiv 3(-2)(16 \cdot 11 \cdot 7) + 10 \cdot 5(17 \cdot 11 \cdot 7) + 4 \cdot 1(17 \cdot 16 \cdot 7) + 0 \pmod{20944} \\
\equiv -7392 + 65450 + 7616 \equiv 65674 \equiv 2842 \pmod{20944}.
\]

Therefore, the least number of coins in the chest is 2842.

2. (a) Since 23 is a prime and 444 = 20(23 - 1) + 4, we have by Fermat’s Theorem that \( 4^{23} \equiv 4 \pmod{23} \). Now \( 4^2 \equiv 4(64) \equiv 4(-5) \equiv -20 \equiv 3 \pmod{23} \), so \( 4^{23} \equiv 4 \pmod{23} \). Thus, \( \text{rem}(4^{444}, 23) = 3 \).

(b) Since 31 is prime and 222 = 7(31 - 1) + 12, we have by Fermat’s Theorem that \( 3^{222} \equiv 3^{12} \pmod{31} \). Now \( 3^4 \equiv 81 \equiv -12 \pmod{31} \), so \( 3^{8} \equiv (-12)^2 \equiv -11 \pmod{31} \), and hence \( 3^{12} = 3^{8} \cdot 3^{4} \equiv -11(-12) \equiv 8 \pmod{31} \). Thus, \( \text{rem}(3^{222}, 31) = 8 \).

(c) Since 17 is prime and 1234 = 77(17 - 1) + 2, we have \( 5^{1234} \equiv 5^2 \equiv 25 \equiv 8 \pmod{17} \), so \( \text{rem}(5^{1234}, 17) = 8 \).

3. Suppose \( p \) is an odd prime factor of \( m = 3^{31} - 1 \). Then, since 31 is prime and \( p \) does not divide \( 3 - 1 = 2 \), we have by Corollary 2 of Fermat’s Theorem that \( p \) has the form \( p = 1 + 3k' \), for some integer \( k' \). Moreover, since \( p \) is odd, then \( k' = 2k \) has to be even, so \( p \) has the form \( p = 1 + 62k \), for some integer \( k \). For \( k = 1, \ldots, 11 \) this yields the (smallest) possibilities \( p = 63, 125, 187, 249, 311, 373, 435, 497, 559, 621, 683 \). Of these, only 3 are prime, so the list reduces to \( p = 311, 373, 683 \). For these we now check whether \( p | 3^{31} - 1 \), or equivalently, whether \( 3^{31} \equiv 1 \pmod{p} \). By the cancellation theorem, this is equivalent to the condition that \( 3^{32} \equiv 3 \pmod{p} \), which is easier to check. Now:

(i) \( 3^8 = 6561 \equiv 30 \pmod{311} \), so \( 3^{16} \equiv -33 \pmod{311} \), and hence \( 3^{32} \equiv (-33)^2 \equiv -155 \equiv 3 \pmod{311} \). Thus, 311 does not divide \( m = 3^{31} - 1 \). [Alternately: use the power-mod algorithm to find that \( \text{rem}(3^{31}, 311) = 52 \neq 1 \).]

(ii) Similarly, \( 3^8 \equiv -153 \pmod{373} \), so \( 3^{16} \equiv -90 \pmod{373} \), and hence \( 3^{32} \equiv (-90)^2 \equiv -106 \pmod{373} \). Thus, 373 is also not a divisor of \( m \). [Here \( \text{rem}(3^{31}, 373) = 89 \).]

(iii) Next we have \( 3^8 \equiv -269 \pmod{683} \), and \( 3^{16} \equiv (-269)^2 \equiv -37 \pmod{683} \), and so \( 3^{32} \equiv 3 \pmod{683} \). Thus, \( p = 683 \) is the smallest odd prime divisor of \( m = 3^{31} - 1 \).
4. Since $340 = 34(11 - 1)$, we see by Corollary 1 of Fermat’s Theorem that $2^{340} \equiv (2^{(11-1)})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$. Moreover, since $340 = 11(31 - 1) + 10$, we see similarly that $2^{340} \equiv 2^{10}(2^{(31-1)})^{11} \equiv 2^{10}1^{11} \equiv (2^5)^2 \equiv (-1)^2 \equiv 1 \pmod{31}$. Thus $2^{340} \equiv 1 \pmod{11}$ and $2^{340} \equiv 1 \pmod{31}$, and so $2^{340} \equiv 1 \pmod{11 \cdot 31}$ by Fact 3 of section 2.6. Since $11 \cdot 31 = 341$, this means that 341 is a pseudoprime to the base 2.

5. Recall that the binomial formula states:

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = (x + y)^n.$$ 

Substituting $x = y = 1$ in this formula yields

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = (1 + 1)^n = 2^n.$$

Similarly, substituting $x = 1$ and $y = -1$ yields

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = (1 + (-1))^n = 0^n = 0.$$ 

6. See the MAPLE solution on the course Web site (www.mast.queensu.ca/~math211).