Math 211

Assignment 6 - Solutions

[5] 1. Let x denote the number of coins in the chest. We then have the following conditions:

$$\begin{array}{rclcrcl} x & \equiv & 3 \pmod{17} & \qquad & x & \equiv & 10 \pmod{16} \\ x & \equiv & 4 \pmod{11} & \qquad & x & \equiv & 0 \pmod{7}. \end{array}$$

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. (Remember to check this!) Here $m = 17 \cdot 16 \cdot 11 \cdot 7 = 20944$, and

$$\begin{array}{rclcl c rclclr} m_1' & = & \frac{17\cdot16\cdot11\cdot7}{17} & = & 16 \cdot 11 \cdot 7, & \qquad & m_1' & \equiv & (-1)(-6)7 & \equiv & 8 & \pmod{17} \\ m_2' & = & \frac{17\cdot16\cdot11\cdot7}{16} & = & 17 \cdot 11 \cdot 7, & & m_2' & \equiv & 1(-5)7 & \equiv & -3 & \pmod{16} \\ m_3' & = & \frac{17\cdot16\cdot11\cdot7}{11} & = & 17 \cdot 16 \cdot 7, & & m_3' & \equiv & 6 \cdot 5(-4) & \equiv & 1 & \pmod{11} \\ m_4' & = & \frac{17\cdot16\cdot11\cdot7}{7} & = & 17 \cdot 16 \cdot 11, & & m_4' & \equiv & 3 \cdot 25 \cdot 4 & \equiv & 3 & \pmod{7}. \end{array}$$

By inspection we see: $\left\{ \begin{array}{rlcrcrl} 8m_1^* & \equiv 1 \pmod{17} & \Rightarrow & m_1^* & \equiv & -2 & \pmod{17} \\ (-3)m_2^* & \equiv 1 \pmod{16} & \Rightarrow & m_2^* & \equiv & 5 & \pmod{16} \\ 1m_3^* & \equiv 1 \pmod{11} & \Rightarrow & m_3^* & \equiv & 1 & \pmod{11} \\ 3m_4^* & \equiv 1 \pmod{7} & \Rightarrow & m_4^* & \equiv & -2 & \pmod{7}. \end{array} \right.$

Thus, since here $a_1 = 3, a_2 = 10, a_3 = 4, a_4 = 0$, we get

$$\begin{array}{rcl} x & \equiv & a_1 m_1^* m_1' + a_2 m_2^* m_2' + a_3 m_3^* m_3' \pmod{m} \\ & \equiv & 3(-2)(16 \cdot 11 \cdot 7) + 10 \cdot 5(17 \cdot 11 \cdot 7) + 4 \cdot 1(17 \cdot 16 \cdot 7) + 0 \pmod{20944} \\ & \equiv & -7392 + 65450 + 7616 \equiv 65674 \equiv 2842 \pmod{20944}. \end{array}$$

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

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

(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 $3^4 = 81 \equiv -12 \pmod{31}$, 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, $\mathrm{rem}(3^{222}, 31) = 8$.

(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 $\mathrm{rem}(5^{1234}, 17) = 8$.

(d) Since $21 = 3\cdot7$ is the product of two distinct primes, we can apply Corollary 3 of Fermat's Theorem. Here $k = (p-1)(q-1) = 2\cdot6 = 12$. Now $\mathrm{rem}(236, 12) = 8$, so applying Corollary 3 with $a = 229 \equiv 1 \pmod{12}$, we get $5^{236} = 5^{229} \cdot 5^7 \equiv 5 \cdot 5^7 \equiv 5^8 \pmod{21}$. Now $5^2 \equiv 4 \pmod{21}$, so $5^8 \equiv (5^2)^4 \equiv 4^4 \equiv (-5)^2 \equiv 4 \pmod{21}$. Thus, $\mathrm{rem}(5^{236}, 21) = 4$.

[3] 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 $p = 1 + 31k'$, 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) $3^8 = 81^2 = 6561 \equiv 30 \pmod{311}$, so $3^{16} \equiv -33 \pmod{311}$, and hence $3^{32} \equiv (-33)^2 \equiv -155 \not\equiv 3 \pmod{311}$. Thus, 311 does not divide $m = 3^{31} - 1$. [Alternately: use the power-mod algorithm to find that $\mathrm{rem}(3^{31}, 311) = 52 \neq 1$.]

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

(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 $m = 3^{31} - 1$.

[3] 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.

By a similar reasoning as above we have $3^{340} \equiv 1^{34} \equiv 1 \pmod{11}$ and $3^{340} \equiv 3^{10}1^{11} \equiv 3 \cdot (3^3)^3 \equiv 3(-4)^3 \equiv -6 \equiv 25 \pmod{31}$ (because $(-4)^3 \equiv -64 \equiv -2 \pmod{31}$). Thus, $3^{340} \not\equiv 1 \pmod{31}$, and hence also $3^{340} \not\equiv 1 \pmod{341}$. (In fact, the Chinese Remainder Theorem shows that $3^{340} \equiv 56 \pmod{341}$, but we don't need to know this.) Thus 341 is not a pseudoprime to the base 3. From this it follows that 341 is not prime because if $n = 341$ were prime, then by Fermat we would have $3^{n-1} \equiv 1 \pmod{n}$, which is false.

[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

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

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