Math 211

Assignment 6

Due 12 November 2021

[5] 1. (Ancient Chinese Problem) A gang of 17 bandits stole a chest of gold coins. When they tried to divide the coins equally among themselves, there were three left over. This caused a fight in which one of the bandits was killed. When the remaining bandits tried to divide the coins again, there were ten left over. Another fight started, and five of the bandits were killed. When the survivors divided the coins, there were four left over. Another fight ensued in which four bandits were killed. The survivors then divided the coins equally among themselves, with none left over. What is the smallest possible number of coins in the chest?

[4] 2. Combine Fermat's Theorem with the power-mod algorithm to find the following remainders by hand:

(a) $\text{rem}(4^{444}, 23)$; (b) $\text{rem}(3^{222}, 31)$; (c) $\text{rem}(5^{1234}, 17)$. (d) $\text{rem}(5^{236}, 21)$.

[3] 3. Use Fermat's method to find (by hand) the smallest odd prime factor p of the number $m = 3^{31} - 1$. Be sure to justify that the p you found is actually a factor of m, and that there are no smaller factors.

[3] 4. Compute $\text{rem}(2^{340}, 11)$ and $\text{rem}(2^{340}, 31)$ and use this to show that 341 is a pseudoprime to the base 2. Moreover, compute $\text{rem}(3^{340}, 31)$ and conclude that 341 is not a pseudoprime to the base 3. (Explain and justify your calculations.)

[2] 5. Verify that the following two identities hold for any $n \geq 1$:

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

[3] 6. MAPLE problem (refer to the MAPLE instruction sheet):

The MAPLE command `chrem(a,m)` uses CRT to solve the simultaneous congruence $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq r$. Here `a`$= [a_1, \ldots, a_r]$ and `m`$= [m_1, \ldots, m_r]$ are the list of coefficients and the list of moduli, respectively. Use this command to solve each of the following simultaneous congruences:

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \\ x &\equiv 6 \pmod 9 \end{aligned} \qquad \text{and} \qquad \begin{aligned} 3x &\equiv 2 \pmod 4 \\ 2x &\equiv 3 \pmod 5 \\ 4x &\equiv 5 \pmod 7 \\ 5x &\equiv 6 \pmod 9 \end{aligned}$$

Explain how you applied the command. Moreover, check (using MAPLE) that the solution you found is actually correct, i.e. that it satisfies the given simultaneous congruences.