1. Use modular arithmetic to determine the day of the week 1000 days after Friday, March 11, 2016.

$$1000 = (142)(7) + 6 \implies 1000 \equiv 6 \bmod 7$$

It will be 6 days after Friday, which is Thursday.

2. Use modular arithmetic to determine the day of the week on March 11, 2036.

There are $(36 - 16)(365) + 5 = 7305$ days between March 11, 2016 and March 11, 2036. We know $7305 \equiv 4 \bmod 7$, so it will be 4 days after Friday, which is Tuesday.

3. Can modular arithmetic be used to help us determine what month it is exactly 5000 days after Friday, March 11, 2016? If so, what month is it? Otherwise, explain why modular arithmetic provides no help in solving this problem.

Modular arithmetic can be used to help solve the problem, but it cannot be used alone. Since months vary in the number of days, we need to know how many days are in each month. We can use mod arithmetic to calculate how many years go by.

$$5000 = 365(13) + 255 \implies 13 \text{ days from now.}$$

March 24 and three leap years leaves us with March 27 and 252 days. From here, we can use a calendar to determine that the day should be sometime in December.

4. Without using a calculator,

find the remainder when 8^{10} is divided by 11 and when 5^9 is divided by 13.

$$\begin{aligned}
10 &= 5 \cdot 2 \\
8^{10} &= 8^{5 \cdot 2} \\
64^5 &\equiv 2^5 \bmod 11 \\
&\equiv 32 \bmod 11 \\
&\equiv 1 \bmod 11
\end{aligned}$$

The remainder is 1.

$$\begin{aligned}
5^9 &= 5^3 \cdot 5^6 \\
5^9 &\equiv 125 \cdot 5^6 \bmod 13 \\
&\equiv -8 \cdot 5^6 \bmod 13 \\
&\equiv 5 \cdot 5^6 \bmod 13 \\
&\equiv 5 \cdot 125 \cdot 125 \bmod 13 \\
&\equiv 125 \bmod 13 \\
&\equiv 5 \bmod 13
\end{aligned}$$

The remainder is 5.

5. If $a \in \mathbb{Z}$, prove that $a^3 \not\equiv 2 \bmod 4$.

Since $a \in \mathbb{Z}$, we have that $a \equiv 0 \bmod 4$, $a \equiv 1 \bmod 4$, $a \equiv 2 \bmod 4$, or $a \equiv 3 \bmod 4$. If $a \equiv 0 \bmod 4$, then $a^3 \equiv 0^3 \bmod 4$, which is equivalent to $0 \bmod 4$. If $a \equiv 1 \bmod 4$, then $a^3 \equiv 1^3 \bmod 4$, which is equivalent to $1 \bmod 4$. If $a \equiv 2 \bmod 4$, then $a^3 \equiv 2^3 \bmod 4$, which is equivalent to $8 \bmod 4$,or $0 \bmod 4$. If $a \equiv 3 \bmod 4$, then $a^3 \equiv 3^3 \bmod 4$, which is equivalent to $27 \bmod 4$, or $1 \bmod 4$. Therefore, it is impossible that $a^3 \equiv 2 \bmod 4$.

$\triangle$

6. Suppose that $m, n \in \mathbb{Z}$, with $m, n \geq 2$ and write $l = lcm(m, n)$.

(a) If a and b are integers such that $a \equiv b \bmod l$, prove that $a \equiv b \bmod m$ and $a \equiv b \bmod n$.

Suppose $a \equiv b \bmod l$. Then $l \mid (a - b)$, or $a - b = lj$, $j \in \mathbb{Z}$. Since $l = lcm(m, n)$, we know that both the prime factorization of m and n appear in the prime factorization of l. Suppose, without loss of generality, that we factor out the prime factorization of $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \in \mathbb{Z}$ out of the prime factorization of $l = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_q^{\gamma_q}$, $q \in \mathbb{Z}$. Then we are left with $l = m \cdot \frac{l}{m}$, where $\frac{l}{m} \in \mathbb{Z}$. Then we have $a - b = m \cdot \frac{l}{m} \cdot j$, which is m times an integer r. Therefore $a - b = mr$, so $m \mid (a - b)$, and $a \equiv b \bmod m$.

$\triangle$

(b) If a and b are integers such that $a \equiv b \bmod m$ and $a \equiv b \bmod n$, can we conclude that $a \equiv b \bmod l$? Either prove your answer or provide a counterexample.

> Since $a \equiv b \bmod m$, we know that $m \mid (a-b)$, and since $a \equiv b \bmod n$, we know that $n \mid (a-b)$. This implies that $a-b$ is a common factor of both m and n, so $l = lcm(m,n)$ is also divisible by $a-b$.

$\triangle$

7. If $a, b, n \in \mathbb{Z}$, we adopt the notation that

$$a + n\mathbb{Z} = \{a + nz \ : \ z \in \mathbb{Z}\}.$$

If $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) \neq \emptyset$, prove that $a + n\mathbb{Z} = b + n\mathbb{Z}$.

> Suppose we have a $w \in (a+n\mathbb{Z}) \cap (b+n\mathbb{Z})$. Then, by definition of $a+n\mathbb{Z}$, $w = a+nz_1$, and, by definition of $b+n\mathbb{Z}$, $w = b+nz_2$. We can say that $a+nz_1 = b+nz_2$, or that $a-b = nz_2 - nz_1$. Consider the case where we take an $x \in a + n\mathbb{Z}$. Then, by definition of $a+n\mathbb{Z}$, we have that $x = a+nz_3$. We can rearrange $a-b = nz_2 - nz_1$ in terms of a so that $a = b+nz_2-nz_1$. Then $x = b + nz_2 - nz_1 + nz_3$, or $x = b + n(z_2 - z_1 + z_3)$. Then $x \in b + n\mathbb{Z}$. Similarly, we can take a $y \in b + n\mathbb{Z}$. Then $y = b + nz_4$ and $b = a + nz_1 - nz_2$, so $y = a + nz_1 - nz_2 + nz_4$. Therefore $y = a + n(z_1 - z_2 + z_4)$ which implies that $y \in a + n\mathbb{Z}$.

$\triangle$

8. If $a, b, n \in \mathbb{Z}$ with $n \geq 2$, prove that the following statements are equivalent.

i $a \equiv b \bmod n$

ii $a \in b + n\mathbb{Z}$

iii $b \in a + n\mathbb{Z}$

Conclude that $a + n\mathbb{Z} = \{x \in \mathbb{Z} \ : \ a \equiv x \bmod n\}$.

> $\underline{(i) \implies (ii)}$ Suppose $a \equiv b \bmod n$. Then $n \mid (a-b)$, so $a - b = nk,\ k \in \mathbb{Z}$. Then $a = b + nk$, so $a \in b + n\mathbb{Z}$ by definition.
>
> $\underline{(ii) \implies (iii)}$ Suppose $a \in b + n\mathbb{Z}$. Then $a = b + nz,\ z \in \mathbb{Z}$, and $a - b = nz$. Then $b = a + n(-z)$, so $b \in a + n\mathbb{Z}$.
>
> $\underline{(iii) \implies (i)}$ Suppose $b \in a + n\mathbb{Z}$. Then $b = a + nz,\ z \in \mathbb{Z}$, so $a - b = -nz$, or $a - b = n(-z)$. Then $n \mid (a-b)$, and $a \equiv b \bmod n$ by definition.
>
> By the transitive property of implication, we are done.
>
> Let $x \in a + n\mathbb{Z}$. Then by properties (iii) and (i), $a \equiv x \bmod n$. Let $y \in \{x \in \mathbb{Z} \ : \ a \equiv x \bmod n\}$. Then by properties (i) and (iii), we have that $y \in a + n\mathbb{Z}$.

$\triangle$