Problem Solutions

1. Show that $10! \equiv -1 \pmod{11}$. (Hint: For $2 \leq a \leq 9$, what is the inverse of a modulo 11?)

Solution. First, notice that we can pair the integers between 2 and 9 so that the integers in each pair are inverses of each other modulo 11. Indeed,

$$\begin{aligned} 2 \cdot 6 = 12 &\equiv 1 \pmod{11} \\ 3 \cdot 4 = 12 &\equiv 1 \pmod{11} \\ 5 \cdot 9 = 45 &\equiv 1 \pmod{11} \\ 7 \cdot 8 = 56 &\equiv 1 \pmod{11}. \end{aligned}$$

So $10! = 10 \cdot 9 \cdot 8 \cdots 2 \cdot 1 = 10(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \equiv 10 \pmod{11}$. Since $10 \equiv= -1 \pmod{11}$, this completes the proof.

2. Check that in the proof of the Chinese Remainder Theorem, the number produced satisfies the desired congruences. Then use the construction of the proof to find all solutions to the system of congruences $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, and $x \equiv 3 \pmod 5$.

Solution. Given a system of congruences $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq n$, the solution given by the Chinese Remainder Theorem is the number $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$, where $M_k = (m_1 m_2 \cdots m_n)/m_k$ and y_k is an inverse of M_k modulo m_k. If we consider x modulo m_i, notice that m_i divides M_k for $k \neq i$, so $x \equiv a_i M_i y_i \pmod{m_i}$. By the choice of y_i, $M_i y_i \equiv 1 \pmod{m_i}$, so this gives $x \equiv a_i \pmod{m_i}$, as desired.

Now, for the system of congruences given here, $M_1 = 20$, $M_2 = 15$ and $M_3 = 12$. $M_1 \equiv 2 \pmod 3$, so an inverse is $y_1 = 2$. $M_2 \equiv 3 \pmod 4$, so an inverse is $y_2 = 3$. $M_3 \equiv 2 \pmod 5$, so an inverse is $y_3 = 3$. So $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 20 \cdot 2 + 15 \cdot 3 + 3 \cdot 12 \cdot 3$ satisfies the desired congruences. The solutions to the system of congruences are exactly the integers congruent to x modulo $3 \cdot 4 \cdot 5$.

3. Let p be prime and suppose $p \nmid a$. For $1 \leq j \leq p-1$, what is an inverse of a^j modulo p?

Solution. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$. So if $k = p - 1 - j$, then a^k is an inverse of a^j modulo p, since $a^j a^k = a^{j+k} = a^{j+p-1-j} = a^{p-1}$.

4. Find a formula for

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$$

and prove it using induction.

Solution. We claim that $1/2 + 1/4 + \cdots + 1/2^n = (2^n - 1)/2^n$.

Base case: (n=1) $1/2 = (2^1 - 1)/2^1$.

Inductive step: Suppose that for some $k \geq 1$, $1/2 + 1/4 + \cdots + 1/2^k = (2^k - 1)/2^k$. Then

$$\begin{aligned}
\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^k}+\frac{1}{2^{k+1}} &= \left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^k}\right)+\frac{1}{2^{k+1}} \\
&= \frac{2^k-1}{2^k}+\frac{1}{2^{k+1}} && \text{by the inductive hypothesis} \\
&= \frac{2(2^k-1)+1}{2^{k+1}} \\
&= \frac{2^{k+1}-1}{2^{k+1}}.
\end{aligned}$$

5. Use induction to show that if A is a finite set, $\mathcal{P}(A)$ has $2^{|A|}$ elements.

Solution. We show this by induction on the size of A.

Base case: If $|A| = 0$, then $A = \emptyset$ and $\mathcal{P}(A) = \{\emptyset\}$. So $\mathcal{P}(A)$ has $1 = 2^0$ elements.

Inductive step: Suppose $|\mathcal{P}(B)| = 2^{|B|}$ for $|B| = k$, and suppose A is a set of cardinality $k+1$. To use induction, we need to relate the subsets of A to the subsets of a set of a smaller size. Let $a \in A$ (such an element exists because $k+1 > 0$), and let A' denote $A - \{a\}$.

Note that all subsets of A are either subsets of A' or are of the form $X \cup \{a\}$ for some subset X of A'. We will pair each subset X of A' with $X \cup \{a\}$; note that every subset of A appears in exactly one pair. This means that for each subset of A', there are two subsets of A. In other words, A has twice as many subsets as A'. This means $|\mathcal{P}(A)| = 2 \cdot |\mathcal{P}(A')| = 2 \cdot 2^k$, where the last equality is by the inductive hypothesis. Simplifying, we get $|\mathcal{P}(A)| = 2^{k+1} = 2^|A|$.

6. Show by induction that $n^2 - 1$ is divisible by 8 whenever n is an odd positive integer.

Solution. To use induction, we write $n = 2k+1$ and induct on k.

Base case: For $k = 0$, $n = 1$ and $1^2 - 1 = 0$, which is divisible by 8.

Inductive step: Suppose for some $l \geq 0$, $(2l+1)^2 - 1$ is divisible by 8. The next odd number is $2(l+1)+1 = 2l+3$; we would like to show $(2l+3)^2 - 1$ is divisible by 8.

$$\begin{aligned}
(2l+3)^2 - 1 &= 4l^2 + 12l + 9 - 1 \\
&= (4l^2 + 4l) + 8l + 8 \\
&= [(2l+1)^2 - 1] + 8(l+1).
\end{aligned}$$

By the inductive hypothesis, the first term is divisible by 8; the second term is clearly divisible by 8, so the entire expression is divisible by 8.