GENERAL INSTRUCTIONS: Use definitions and theorems we proved in class to explain your answers to all the questions below.

Check all computations carefully. Partial credit will only be given up to your first significant error.

1) (16 points) Find the remainder when

\[ 7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43 \]

is divided by 11.

Answer:

We have

\[ 15 \equiv 4 \pmod{11}, \ 16 \equiv 5 \pmod{11}, \ 17 \equiv 6 \pmod{11} \]

\[ 23 \equiv 1 \pmod{11}, \ 24 \equiv 2 \pmod{11}, \ 25 \equiv 3 \pmod{11}, \ 43 \equiv 10 \pmod{11} \]

Hence

\[ 7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43 \equiv 7 \cdot 8 \cdot 9 \cdot 4 \cdot 5 \cdot 6 \cdot 1 \cdot 2 \cdot 3 \cdot 10 \pmod{11} \]

\[ \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \pmod{11} \]

\[ \equiv 10! \pmod{11} \]

Since 11 is prime we have by Wilson’s theorem

\[ 10! \equiv -1 \pmod{11} \]

Since \(-1 \equiv 10 \pmod{11}\) we have the remainder upon division by 11 is 10.
2) (16 points) Consider the congruence

\[ 12x \equiv c \pmod{30} \]

a) For which integers \( c \), \( 0 \leq c < 30 \), does the congruence have solutions? Explain your answer.
b) For each value of \( c \) you gave in a) give the number of distinct solutions \( (\text{mod } 30) \) that the congruence has.
c) For the largest value of \( c \), \( c < 30 \) that you gave in a) list all of the solutions \( (\text{mod } 30) \).

Answer a):
We have \((12, 30) = 6\). There are solutions when \( 6 \mid c \). So the values of \( c \), \( 0 \leq c < 30 \) that have solutions are

\[ 0, 6, 12, 18, 24 \]

Answer b): For each of the values in a) there are 6 solutions.

Answer c):
For the congruence

\[ 12x \equiv 24 \pmod{30} \]

we have \( x_0 \equiv 2 \) is one solution. Hence the others are

\[ x \equiv x_0 + \frac{30}{6} t \equiv 2 + 5t \pmod{30} \text{ for } 0 \leq t < 6 \]

So the solutions are

\[ 2, 7, 12, 17, 22, 27 \pmod{30} \]
3) (16 points)
a) Find the smallest positive integer that leaves a remainder of 1 when divided by 2 or 5 and is divisible by 3.
b) Describe the set of all integers with the properties in a).
   Give reasons including any theorems you are using.

Answer to a) and b):
The integers that satisfy the properties in a) are the integers \( x \) that satisfy the con-
gruence
\[
\begin{align*}
x &\equiv 1 \pmod{2} \\
x &\equiv 1 \pmod{5} \\
x &\equiv 0 \pmod{3}
\end{align*}
\]
Using the iterative method we have \( x = 1 + 2u \) from the first congruence. Substituting this into the second congruence gives
\[
\begin{align*}
1 + 2u &\equiv 1 \pmod{5} \\
2u &\equiv 0 \pmod{5} \Rightarrow u \equiv 0 \pmod{5}
\end{align*}
\]
So \( u = 5v \) and \( x = 1 + 2u = 1 + 2(5v) = 1 + 10v \). Substituting this into the third congruence gives
\[
\begin{align*}
1 + 10v &\equiv 0 \pmod{3} \\
10v &\equiv -1 \equiv 2 \pmod{3}
\end{align*}
\]
Since \( 10 \equiv 1 \pmod{3} \) this becomes
\[
v \equiv 2 \pmod{3}
\]
So \( v = 2 + 3w \) and \( x = 1 + 10v = 1 + 10(2 + 3w) = 21 + 30w \) where \( w \) is any integer. From this we see that 21 is the smallest positive integer that satisfies the properties, and
\[
\{21 + 30w \mid w \in \mathbb{Z}\} \text{ i.e. } \{ x \mid x \equiv 21 \pmod{30}\}
\]
Note: If one observes that 21 is the smallest positive integer that satisfies the congruences, then since the moduli (i.e. 2, 3, 5) are pairwise relatively prime the set of integers \( x \) that satisfy all the congruences is \( \{x \mid x \equiv 21 \pmod{30}\} \) by the Chinese Remainder Theorem.
4) (16 points) Use congruences ($\mod 9$) to explain what the missing digit is in the following calculation:

$$24,789 \cdot 43,717 = 1,083,\underline{?00},713$$

NOTE: You must explain your answer using congruences ($\mod 9$) in order to receive credit.

Answer:

An integer is congruent to the sum of it’s digits ($\mod 9$) so we have:

$$24,789 \equiv 2 + 4 + 7 + 8 + 9 \pmod{9}$$
$$\equiv 3 \pmod{9}$$

$$43,717 \equiv 4 + 3 + 7 + 1 + 7 \pmod{9}$$
$$\equiv 4 \pmod{9}$$

$$1,083,700,713 \equiv 1 + 8 + 3 + ? + 7 + 1 + 3$$
$$\equiv 5 + ? \pmod{9}$$

Considering the multiplication ($\mod 9$) we have

$$3 \cdot 4 \equiv 5 + ? \pmod{9}$$

Since $12 \equiv 3 \pmod{9}$ this becomes

$$3 \equiv 5 + ? \pmod{9}$$

So we get

$$? \equiv -2 \equiv 7 \pmod{9}$$

Since the only digit $x$, $0 \leq x \leq 9$ that satisfies $x \equiv 7 \pmod{9}$ is $x = 7$ we have the missing digit must be $7$. 
5)(16 points) Let $p$ be a prime number.

a) If

$$a^2 \equiv b^2 \pmod{p}$$

what can you conclude about $a$, $b \pmod{p}$?

b) Prove your answer in a) using the definition and basic properties of congruences and divisibility.

Answer:

a) $a \equiv \pm b \pmod{p}$

b) $a^2 \equiv b^2 \pmod{p} \iff p \mid a^2 - b^2 \iff p \mid (a+b)(a-b)$

Since $p$ is prime we must have $p \mid (a+b)$ or $p \mid (a-b)$ (or both).

If $p \mid (a+b)$ then $a+b \equiv 0 \pmod{p} \Rightarrow a \equiv -b \pmod{p}$.

If $p \mid (a-b)$ then $a-b \equiv 0 \pmod{p} \Rightarrow a \equiv b \pmod{p}$.

This shows

$$a^2 \equiv b^2 \pmod{p} \Rightarrow a \equiv \pm b \pmod{p}$$
6) (16 points) Show that if \( a \) is an integer satisfying \((a, 2520) = 1\) then
\[
a^{12} \equiv 1 \pmod{2520}
\]
State any theorems you are applying.

Answer:
Factoring 2520 we get 2520 = \(2^3 \cdot 3^2 \cdot 5 \cdot 7\). Then, since \(2^3\), \(3^2\), 5, 7 are pairwise relatively prime we have, by the Chinese Remainder Theorem, that \(a^{12} \equiv 1 \pmod{2520}\) if and only if
\[
\begin{align*}
a^{12} &\equiv 1 \pmod{2^3} \\
a^{12} &\equiv 1 \pmod{3^2} \\
a^{12} &\equiv 1 \pmod{5} \\
a^{12} &\equiv 1 \pmod{7}
\end{align*}
\]
(This will be explained precisely below).
We consider each congruence separately.
\(\pmod{2^3}\)
\((a, 2520) = 1 \Rightarrow (a, 2^3) = (a, 8) = 1. \ \phi(8) = 4\) where \(\phi\) is the Euler phi function. By Euler’s Theorem
\[
a^4 \equiv 1 \pmod{2^3}
\]
Cubing both sides gives
\[
a^{12} \equiv 1 \pmod{2^3}
\]
\(\pmod{3^2}\)
\((a, 2520) = 1 \Rightarrow (a, 3^2) = (a, 9) = 1. \ \phi(9) = 6\) where \(\phi\) is the Euler phi function. By Euler’s Theorem
\[
a^6 \equiv 1 \pmod{3^2}
\]
Squaring both sides gives
\[
a^{12} \equiv 1 \pmod{3^2}
\]
\(\pmod{5}\)
\((a, 2520) = 1 \Rightarrow (a, 5) = 1. \ \)By Fermat’s Little Theorem
\[
a^4 \equiv 1 \pmod{5}
\]
Cubing both sides gives
\[
a^{12} \equiv 1 \pmod{5}
\]
\(\pmod{7}\)
\((a, 2520) = 1 \Rightarrow (a, 7) = 1. \ \)By Fermat’s Little Theorem
\[
a^6 \equiv 1 \pmod{7}
\]
Squaring both sides gives
\[
a^{12} \equiv 1 \pmod{7}
\]
The above shows that the integer $a^{12}$ satisfies the system of congruences

\[
\begin{align*}
x &\equiv 1 \pmod{2^3} \\
x &\equiv 1 \pmod{3^2} \\
x &\equiv 1 \pmod{5} \\
x &\equiv 1 \pmod{7}
\end{align*}
\]

and the integer 1 also obviously satisfies this system of congruences. Since the moduli are relatively prime, by the Chinese Remainder Theorem there is a unique solution modulo the product, i.e. $(mod\ 2520)$. Since $a^{12}$ and 1 are both solutions we must have

\[
a^{12} \equiv 1 \pmod{2520}
\]