Fermat's Little Theorem and Chinese Remainder Theorem Solutions

Notation:

$a$ divides $b$: $a|b$

$a$ does not divide $b$: $a \not| b$

(1)

$$\begin{aligned}
f(n) &\equiv 5n + 9an \pmod{13} \\
&\equiv (5+9a)n \pmod{13} \\
&\equiv 0 \pmod{13} \quad \text{for any } n \text{ and therefore} \\
5 + 9a &\equiv 0 \pmod{13} \\
9a &\equiv 8 \pmod{13} \\
-4a &\equiv 8 \pmod{13} \\
a &\equiv -2 \equiv 11 \pmod{13}
\end{aligned}$$

$$\begin{aligned}
f(n) &\equiv 13n + 9an \pmod{5} \\
&\equiv (3+4a)n \pmod{5} \\
4a &\equiv 2 \pmod{5} \\
a &\equiv 3 \pmod{5}
\end{aligned}$$

If $a \equiv 11 \pmod{13}$, $a \equiv 3 \pmod{5}$, what is $a \equiv ? \pmod{65}$?

$$\begin{aligned}
a &\equiv 33 \pmod{65} \\
a &\equiv 33 \pmod{65}
\end{aligned}$$

(2) If $p = 2$:

$$2^2 + 3^2 = 13^1$$

which cannot be of the form $a^n$ where $n > 1$.

Otherwise, if $p$ is odd:

$$2^p + 3^p = \underbrace{(2+3)}_{5}(2^{p-1} - 2^{p-2} \times 3^1 + 2^{p-3} \times 3^2 + \cdots + 3^{p-1})$$

$$\begin{aligned}
\text{Rightmost factor} &\equiv 2^{p-1} - 2^{p-2} \times 3^1 + 2^{p-3} \times 3^2 + \cdots + 3^{p-1} \pmod{5} \\
&\equiv 2^{p-1} + 2^{p-1} + 2^{p-1} + \cdots + 2^{p-1} \pmod{5} \\
&\equiv p \cdot 2^{p-1} \pmod{5}
\end{aligned}$$

If $p \neq 5$, then we see that the rightmost factor is not divisible by 5, so:

$$5|2^p + 3^p \text{ but } 5^2 \not| 2^p + 3^p$$

$$\Rightarrow 2^p + 3^p \text{ cannot be } a^n \text{ where } a \in \mathbb{Z}, n \in \mathbb{Z}, n > 1.$$

When $p = 5$,

$$\begin{aligned} 2^5 + 3^5 &= 32 + 243 \\ &= 275 \\ &= 5^2 \times 11^1 \quad \text{-also } \neq a^n. \end{aligned}$$

(3)

$$\underbrace{111 \cdots 1}_{k \text{ ones}} = \frac{10^k - 1}{9}$$

When $p = 3$: $111, 111111, 111111111, \ldots$ (where the number of digits is divisible by three) are numbers that are divisible by three.
If $p > 5$: It suffices to show that infinitely many integers of the form $10^k - 1$ where $k \in \mathbb{Z}^+$ are divisible by $p$ since 9 is not divisible by $p$.

$$\begin{aligned} 10^{a(p-1)} &\equiv (10^{p-1})^a \pmod p \\ &\equiv 1^a \equiv 1 \pmod p \quad \text{by FLT since } p > 5 \Rightarrow gcd(10, p) = 1 \\ \text{so} \quad 10^{a(p-1)} - 1 &\equiv 0 \pmod p \quad \text{for any } a \in \mathbb{Z}^+. \end{aligned}$$

Dividing by 9, this gives us infinitely many numbers of the form $11 \cdots 1$ which are divisible by the prime $p$.

(4) $(m, n) = (1, 1)$ is one obvious solution to

$$3^m - 1 = 2^n.$$

It is the only solution for which $n = 1$.
Now suppose $n \geq 2$.

$$3^m - 1 \equiv (-1)^m - 1 \pmod 4$$

Therefore if $(m, n)$ is a solution with $n \geq 2$ so that $4|2^n$, then 4 must divide $3^m - 1 = 2^n$ and the equation above indicates $m$ must be even. This allows us to factor:

$$(3^{m/2} + 1)(3^{m/2} - 1) = 2^n.$$

Thus:
a) $(3^{m/2} + 1)$ and $(3^{m/2} - 1)$ are both powers of 2
b) $(3^{m/2} + 1) - (3^{m/2} - 1) = 2$

What powers of 2 have difference 2? Only $4, 2$. So we must have $3^{m/2} + 1 = 4, 3^{m/2} - 1 = 2$, i.e. $m = 2$.
Therefore $(m, n) = (2, 2)$ is the only solution for which $n \geq 2$.
When $n \leq 0$ it is easy to see there are no solutions in this case.

(5) It suffices to show $n$ must be a power of $p$ in the case where $p \not| a, b$. Write $n = p^r m$ where $p \not| m$.

$$p^k = a^n + b^n = (a^{p^r})^m + (b^{p^r})^m$$

$n$ is odd $\Rightarrow m$ is odd. Therefore we can factor:

$$\begin{aligned} p^k &= a^n + b^n = (a^{p^r})^m + (b^{p^r})^m \\ &= (a^{p^r} + b^{p^r})\left((a^{p^r})^{m-1} - (a^{p^r})^{m-2}b^{p^r} + (a^{p^r})^{m-3}(b^{p^r})^2 - \cdots + (b^{p^r})^{m-1}\right) \quad (*) \end{aligned}$$

Factoring again,

$$\begin{aligned} p^k &= a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b - \cdots + b^{n-1}) \\ \Rightarrow a + b &\equiv 0 \pmod p \quad \text{since } a + b > 1 \\ \Rightarrow b &\equiv -a \mod p \end{aligned}$$

Substituting $b \equiv -a \mod p$ into the righthand factor of $(*)$:

$$\begin{aligned} R.S. &\equiv \left((a^{p^r})^{m-1} - (a^{p^r})^{m-2}b^{p^r} + (a^{p^r})^{m-3}(b^{p^r})^2 - \cdots + (b^{p^r})^{m-1}\right) \pmod p \\ &\equiv (a^{p^r})^{m-1} + (a^{p^r})^{m-1} + \cdots + (a^{p^r})^{m-1} \pmod p \\ &\equiv m(a^{p^r})^{m-1} \pmod p \\ &\not\equiv 0 \pmod p \end{aligned}$$

Therefore in order for the whole product to be a power of $p$, this factor above must equal 1. The only way this is possible is if $m = 1$. Thus, we see that $n = p^r \times m = p^r$.

8) We see that this is true for $p = 2$. Thus we assume $p > 2$.
Suppose $q$ is a prime divisor of $2^p - 1$. Then

$$2^p \equiv 1 \pmod q.$$

Let $d$ be the smallest positive integer such that

$$2^d \equiv 1 \pmod q.$$

Then if $2^a \equiv 1 \mod q$, then $d|a$.
(This is true since if $d$ does not divide $a$, then $a = cd + r$ where $1 \le r \le d - 1$–think of $r$ as the remainder when you divide $a$ by $d$. Then

$$1 \equiv 2^a \equiv 2^{cd} \cdot 2^r \equiv 2^r \pmod q \Rightarrow 2^r \equiv 1 \pmod q$$

but $r < d$ and $d$ was supposed to be the smallest such integer–contradiction.)
Thus $d|p$. Observe that $d \neq 1$, and so $d = p$.
Now by Fermat's Little Theorem, $2^{q-1} \equiv 1 \pmod q$, so $d = p$ divides $q - 1$. This implies that $p \le q - 1$, so $q > p$.
A consequence of this result is the fact that there are infinitely many prime numbers. This was known by the mathematicians of ancient Greece.

9) $n = 1:$ 1, 2 work
$n = 2:$ 512 works
Assume by induction that we've found $k$ such that the last $N$ digits of $2^k$ are 1s and 2s. Let's construct another number whose last $N + 1$ digits are 1s and 2s from this number. We can also assume by induction that $k > N$.

$$2^k = a10^N + b$$

where $b$ is an $N$-digit number consisting of 1s and 2s.

$$\text{Let } r := \phi(5^N) = 5^N - 5^{N-1} = 4 \cdot 5^{N-1}.$$

(Note: the Euler phi function counts the number of integers between 1 and $5^N$ with gcd 1 with $5^N$.)

By Euler-Fermat's Theorem,

$$2^r \equiv 1 \pmod{5^N}.$$

Now $2^k, 2^{k+r}, 2^{k+2r}, \ldots, 2^{k+4r}$ all have $b$ as last $N$ digits: in order to show this, we only need to show that they are congruent modulo $2^N$ and $5^N$ so that they are congruent modulo $10^N$.

Congruent mod $2^N$: $k > N$ and so $2^k, 2^{k+r}, \ldots, 2^{k+4r}$ are all $\equiv 0$ mod $2^N$

Congruent mod $5^N$: $2^r \equiv 1 \pmod{5^N}$ so $2^{k+r} \equiv 2^k \cdot 1 \equiv 2^k \pmod{5^N}$ etc.

Claim: $N + 1^{\text{st}}$ digits different for above five numbers.

Proof: If two are the same, then $2^{k+cr} \equiv 2^{k+dr} \pmod{5^{N+1}}$ where $c > d$

$$\text{then} \quad \underbrace{2^{k+dr}}_{\text{no factors of 5}} \times \underbrace{\left(2^{(c-d)r} - 1\right)}_{\underbrace{(2^r - 1)}_{\substack{5^N | 2^r - 1 \text{ (FLT)} \\ \text{but } 5^{N+1} \nmid 2^r - 1 \\ \text{by induction}}} \times \underbrace{\left((2^r)^{c-d-1} + (2^r)^{c-d-2} + \cdots + 1\right)}_{\equiv 1 + 1 + \cdots + 1 \equiv c - d \pmod 5}} \equiv 0 \pmod{5^{N+1}}$$

$$\begin{aligned} \text{Thus} \quad 2^{k+cr} &\equiv 2^{k+dr} \pmod{5^{N+1}} \\ \Rightarrow c &\equiv d \pmod 5 \end{aligned}$$

Thus $2^k, 2^{k+r}, \ldots, 2^{k+4r}$ leave different residues modulo $5^{N+1}$ and so their $N + 1^{\text{st}}$ digits are distinct.

Now the five numbers are divisible by $2^k > 2^N$

$$\begin{aligned} \Rightarrow \text{ the } N + 1^{\text{st}} \text{ digits are :} \quad & 0, 2, 4, 6, 8 \\ \text{or} \quad & 1, 3, 5, 7, 9 \end{aligned}$$

in some order.

$\Rightarrow$ one of the numbers $2^{k+cr}$ only has 1s and 2s as its last $N+1$ digits. If $k+cr \leq N+1$, we can repeat the above process until we get some $k + cr > N + 1$.