1.

(a) Use Fermat's little theorem to find the remainder when $(116)^{54}$ is divided by 11.

Hint: First find the least residue of $116 \bmod 11$, and work with that instead of 116. Smaller numbers lead to easier calculations!

(b) Prove that $a^{13} \equiv a \bmod 91$ for all $a \in \mathbb{Z}$. Note that $273 = 3 \cdot 7 \cdot 13$.

(a) By FLT, we have $a^{10} \equiv 1 \bmod 11$ for any integer a not divisible by 11. Also note that $116 \equiv 6 \bmod 11$.

So $(116)^{54} \equiv 6^{54} \equiv 6^{5\cdot10+4} \equiv (6^{10})^5 6^4 \equiv 1^5 \cdot 36^2 \equiv 3^2 \equiv 9 \bmod 11$.

(b) $a^{13} \equiv a \bmod 91$ if and only if $a^{13} - a \equiv 0 \bmod 91$, if and only if $91|(a^{13} - a)$, if and only if $7|(a^{13} - a)$ and $13|(a^{13} - a)$, if and only if $a^{13} - a \equiv 0 \bmod 7$ and $a^{13} - a \equiv 0 \bmod 13$, if and only if $a^{13} \equiv a \bmod 7$ and $a^{13} \equiv a \bmod 13$

In summary, $a^{13} \equiv a \bmod 91$ if and only if $a^{13} \equiv a \bmod 7$ and $a^{13} \equiv a \bmod 13$.

Let $p = 7$ or 13. We need to show that $a^{13} \equiv a \bmod p$. This is clearly true if $a \equiv 0 \bmod p$, so assume $(a, p) = 1$.

By FLT, $a^{7-1} \equiv 1 \bmod 7$, so $a^{13} \equiv a^{1+6\cdot2} \equiv a \cdot (a^6)^2 \equiv a \cdot 1^2 \equiv a \bmod 7$.

By FLT, $a^{13-1} \equiv 1 \bmod 13$, so $a^{13} \equiv a^{1+12} \equiv a \cdot a^{12} \equiv a \cdot 1 \equiv a \bmod 13$.

2. Let p be a prime. Use Fermat's little theorem to prove

(a) $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \bmod p$.

(b) $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \bmod p$

Since $(k, p) = 1$ for $1 \le k \le p-1$, we can use FLT to get

(a) $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv 1 + 1 + \ldots 1 \equiv p - 1 \equiv -1 \bmod p$.

(b) $1^p + 2^p + \ldots + (p-1)^p \equiv 1 + 2 + 3 + \ldots + (p-1) \equiv \frac{(p-1)(p-1+1)}{2} \equiv p\left(\frac{p-1}{2}\right) \bmod p$. Since p is odd, $\frac{p-1}{2}$ is an integer, so $p\left(\frac{p-1}{2}\right) \equiv 0 \bmod p$.

3. Let a be an integer coprime to 7. Prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

$(a^3 - 1)(a^3 + 1) = a^{7-1} - 1 \equiv 0 \bmod 7$ by FLT. So $7|(a^3 - 1)(a^3 + 1)$. Thus by Euclid's Lemma, $7|(a^3 - 1)$ or $7|(a^3 + 1)$.

4. Use Wilson's Theorem to find the least residue of $6(25)! \bmod 29$.

For $a = 26, 27, 28$, the multiplicative inverse of a modulo 29 exists because $(a, 29) = 1$.

We have $6(25)! \equiv 3\cdot2\cdot(25)!\cdot26\cdot27\cdot28\cdot26^{-1}\cdot27^{-1}\cdot28^{-1} \equiv 3\cdot2\cdot(28)!\cdot(-3)^{-1}\cdot(-2)^{-1}\cdot(-1)^{-1} \bmod 29$.

Now use $28! \equiv -1 \bmod 29$ (Wilson's Theorem), $3 \cdot (-3)^{-1} \equiv -1 \bmod 29$, $2 \cdot (-2)^{-1} \equiv -1 \bmod 29$, $(-1)^{-1} \equiv -1 \bmod 29$.

Conclusion: $6(25)! \equiv 1 \bmod 29$.

Bonus point

5. Let p be a prime. Let a and b be two integers. Prove that if $a^p - b^p$ is divisible by p, then $a^p - b^p$ is divisible by p^2. (So the stronger divisibility condition is automatically true.)

In the language of congruences, we are given that $a^p - b^p \equiv 0 \bmod p$. Fermat's Little Theorem says that $a^p \equiv a \bmod p$ and $b^p \equiv b \bmod p$. Thus what we are given implies that $a \equiv b \bmod p$. So a and b differ by a multiple of p, and we can write $a = b + pk$ for some $k \in \mathbb{Z}$.

Next, write $a^p - b^p = (b + pk)^p - b^p$ and use the Binomial theorem.

$$(b + pk)^p - b^p = b^p + \binom{p}{1} b^{p-1}(pk)^1 + \binom{p}{2} b^{p-2}(pk)^2 + \ldots + \binom{p}{p-1} b^1 (pk)^{p-1} + (pk)^p - b^p.$$

First note that the two occurences of b^p on the right cancel out. In class, we saw that $\binom{p}{\ell} \equiv 0 \bmod p$ for $1 \le \ell \le p-1$. We claim that each term $\binom{p}{\ell} b^{p-\ell}(pk)^{\ell}$ on the right is divisible by p^2 for $1 \le \ell \le p-1$. This is because at least one factor of p comes from $\binom{p}{\ell}$ and at least one factor of p comes from $(pk)^{\ell}$. Also, the last term $(pk)^p$ is divisible by p because $p \ge 2$.

Thus

$$(b+pk)^p - b^p \equiv \cancel{b^p} + 0 + 0 + \ldots + 0 + 0 - \cancel{b^p} \bmod p^2 \implies (b+pk)^p \equiv b^p \bmod p^2 \implies a^p \equiv b^p \bmod p^2.$$