26. *(1 point.)* By Fermat's little theorem, $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv \overbrace{1 + 1 + \cdots + 1}^{p-1} \equiv p - 1 \equiv -1 \bmod p$.

27c. *(1 point.)* By Fermat's little theorem and Wilson's theorem, $(p-1)! + 2^{p-1} \equiv -1 + 1 \equiv 0 \bmod p$.

35. *(3 points.)* $x \equiv 33 \bmod 84$.

$$\begin{aligned} x &= 1 + 4t_1 = 3t_2 = 5 + 7t_3 \\ 3t_2 - 4t_1 = 1 &\Leftrightarrow t_2 = 3 + 4t_4, t_1 = 2 + 3t_4 \\ 4t_1 - 7t_3 = 4 &\Leftrightarrow 12t_4 - 7t_3 = -4 \Leftrightarrow t_4 = 2 + 7t_5, t_3 = 4 + 12t_5 \\ x &= 1 + 4t_1 = 9 + 12t_4 = 33 + 84t_5 \end{aligned}$$

41. *(3 points.)* Assume that, for some integer $k \geq 0$, we have either

$$\frac{m}{n} = 10^k(0.\overline{a_1 a_2 \ldots a_h}) = 10^k \frac{a_1 \ldots a_h}{10^h - 1}, \quad \text{or} \quad 10^k \frac{m}{n} = 0.\overline{a_1 a_2 \ldots a_h} = \frac{a_1 \ldots a_h}{10^h - 1},$$

that is

$$(10^h - 1)m = (10^k n)a_1 \ldots a_h \quad \text{or} \quad 10^k(10^h - 1)m = n(a_1 \ldots a_h).$$

Then $m \mid a_1 \ldots a_h$, provided $(m, 10^k n) = 1$ in the first case, or $(m, n) = 1$ in the second. (If $bm = an$ and $mx + ny = 1$ then $m(ax + by) = max + mby = max + any = a(mx + ny) = a$, hence m divides a.)

If such k does not exist, or if $(m, 10^k n) > 1$, then m does not necessarily divide $a_1 \ldots a_n$. For example, $6/18 = 0.333\ldots$, but $6 \nmid 3$; $20/9 = 2.222\ldots$, but $20 \nmid 2$; $15/11 = 1.36\ldots$ contains the cycle 36, but $15 \nmid 36$; $234/999 = 0.234234\ldots$ contains the cycle 234, but also the cycles 342 and 423. Note that if $m/n \leq 1$, our assumptions are equivalent to assuming that $k = 0$ and $(m, n) = 1$.

I think we are supposed to assume $m/n = 0.\overline{a_1 a_2 \ldots a_h}$ and $(m, n) = 1$. In this case, apparently by a theorem we have $10^h \equiv 1 \bmod n$, say $10^h - 1 = nn'$. Then $10^h m/n = a_1 \ldots a_h + m/n \Rightarrow n'm = (10^h - 1)m/n = a_1 \ldots a_h$, hence $m \mid a_1 \ldots a_h$.

42. *(4 points.)*

```
je parie que vous avez decode ce message stop
vive les mathematiques
```

1. *(5 points.)*

Supplementary question. Label a deck of $2n$ cards $1, 2, \ldots, 2n$. A perfect shuffle permutes the cards as follows:

$$\begin{array}{lcllcl} 1 & \to & 1 & n+1 & \to & 2 \\ 2 & \to & 3 & n+2 & \to & 4 \\ & \vdots & & & \vdots & \\ i & \to & 2i - 1 & n+i & \to & 2i = 2(n+i) - 1 - (2n-1) \\ n & \to & 2n - 1 & n+n & \to & 2n = 2(n+n) - 1 - (2n-1) \end{array}$$

Note that $m \to \sigma(m) \equiv 2m - 1 \bmod 2n - 1$, $1 \leq m \leq 2n$. After the k-th perfect shuffle, $m \to \sigma^k(m) \equiv 2^k m - 2^{k-1} - \cdots - 1 \equiv 2^k m - (2^k - 1) \bmod 2n - 1$. The deck will be in its original order after k perfect shuffles if and only if

$$\sigma^k(m) = m, \quad \text{iff} \quad 2^k m - (2^k - 1) \equiv m \bmod 2n - 1, \quad \text{iff} \quad (2^k - 1)(m - 1) \equiv 0 \bmod 2n - 1,$$

for each $m \in \{1, 2, \ldots, 2n - 1\}$ ($2n$ is fixed). This holds if and only if $2^k \equiv 1 \bmod 2n - 1$ (for necessity consider $m = 2$), if and only if k is a multiple of the order of 2 modulo $2n - 1$ (which exists because $(2, 2n - 1) = 1$).

Suppose $2n-1 = p_1^{\nu_1}\cdots p_t^{\nu_t}$, the p_i odd primes. By the Chinese Remainder Theorem, $2^a \equiv 1 \bmod 2n-1$ if and only if $2^a \equiv 1 \bmod p_i^{\nu_i}$ for each i, if and only if a is a multiple of $\mathrm{ord}_{p_i^{\nu_i}}(2)$ (the order of 2 modulo $p_i^{\nu_i}$), for each i, if and only if a is a multiple of $[\mathrm{ord}_{p_1^{\nu_1}}(2), \ldots, \mathrm{ord}_{p_t^{\nu_t}}(2)]$ ([,] is the least common multiple).

Now $\mathrm{ord}_{p_i^{\nu_i}}(2)$ divides $\varphi(p_i^{\nu_i}) = (p_i-1)p_i^{\nu_i-1}$. If $2^a \equiv 1 \bmod p_i^{\nu_i}$, then $2^a \equiv 1 \bmod p_i$, so a is a multiple of $p_i - 1$, and $\mathrm{ord}_{p_i^{\nu_i}}(2) = (p_i-1)p_i^r$, for some $r \in \{0, 1, \ldots, \nu_i - 1\}$. In general, we can't say much more than this, for instance $\mathrm{ord}_{3^3}(2) = (3-1)3^{3-1}$, and $\mathrm{ord}_{p^2}(2) = p-1$ if $p = 1093, 3511$. (Can you find another prime p such that $2^{p-1} \equiv 1 \bmod p^2$? Start looking at around 10^{15}.)

To conclude, the smallest k such that k perfect shuffles returns a deck of $2n-1 = p_1^{\nu_1}\cdots p_t^{\nu_t}$ cards to its orginal order is $k = \mathrm{ord}_{2n-1}(2)$, which is at least $[p_1 - 1, \ldots, p_t - 1]$ and at most $[(p_1-1)p_1^{\nu_1-1}, \ldots, (p_t-1)p_t^{\nu_t-1}]$.

Optional 1. This time $m \to \sigma(m) \equiv 2m \bmod 2n+1$:

$$\begin{array}{lcllcl}
1 & \to & 2 & n+1 & \to & 1 \\
2 & \to & 4 & n+2 & \to & 3 \\
 & \vdots & & & \vdots & \\
i & \to & 2i & n+i & \to & 2i-1 = 2(n+i)-(2n+1) \\
n & \to & 2n & n+n & \to & 2n-1 = 2(n+n)-(2n+1)
\end{array}$$

We want k such that $\sigma^k(m) \equiv 2^k m \equiv m \bmod 2n+1$, $1 \le m \le 2n$. This holds if and only if $2^k \equiv 1 \bmod 2n+1$, that is k is a multiple of the order of 2 modulo $2n+1$. If $2n = 52$, then we have to shuffle 52 times in this way to get our deck back in order (for $2n+1 = 53$ is prime). Shuffling the first way, we only have to shuffle $\varphi(51) = (3-1)(17-1) = 32$ times. However, sometimes $\mathrm{ord}_{2n+1}(2) < \mathrm{ord}_{2n-1}(2)$, for example $2^{18} \equiv 1 \bmod 19$, but $2^{12} \equiv 1 \bmod 21$.

Optional 2. If the deck has $2n+1$ cards, we can't split it in half. We can split it so that the last card, $2n+1$, is at the bottom of the left "half", or on the bottom of the right "half". In either case, card $2n+1$ remains fixed at the bottom of the deck after a shuffle. The problem is therefore equivalent to the problem of $2n$ cards.

17 points, plus 3 points for a reasonable attempt at all questions = 20 points.