P. Set 5 Solutions

(1) Identify the 41 colors with the numbers $0, \cdots, 40$. The strategy is as follows:

- The first gnome studies the colors $c_2, c_3, \cdots, c_{1000}$ of all the rest of the gnomes. He guesses
$$(c_2 + c_3 + \cdots c_{1000}) \% 41$$
for his own color. He is probably wrong, but it will be ok! Call his answer s.
- Gnome 2 can see $c_3, \cdots, c_{1000}$. She computes
$$c_3 + \cdots + c_{1000},$$
and subtracts it from s. ~~She~~ The result is $\equiv c_2 \bmod 41$, so she works out c_2 and (correctly) guesses it.
- Gnome 3 knows c_2 (since gnome 2 was correct) as well as $c_4 + \cdots + c_{1000}$ (by observation); she computes $c_2 + c_4 + \cdots + c_{1000}$, subtracts it from s, and obtains a number $\equiv c_3 \bmod 41$, ~~she~~ from which she finds c_3 and (correctly) guesses it.

continuing this way:

- Gnome n knows s as well as $c_2, c_3, \cdots, c_{n-1}$ (by listening) and $c_{n+1}, \cdots, c_{1000}$ (by looking). She computes $c_2 + c_3 + \cdots + c_{n-1} + c_{n+1} + \cdots + c_{1000}$, subtracts it from s, finds the number in $\{0, \cdots, 40\}$ congruent to the result and (correctly) guesses it.

In this way, every gnome but the first is certain to guess correctly.

(2) Observe that $n \equiv -10 \mod (n+10)$.
Hence

$$\begin{aligned}(n+10) \mid (n^3+100) &\iff n^3 \equiv -100 \mod (n+10)\\ &\iff (-10)^3 \equiv -100 \mod (n+10)\\ &\iff 0 \equiv 900 \mod (n+10)\\ &\iff (n+10) \mid 900.\end{aligned}$$

So the largest such n is $900-10 = \boxed{890}$.

(3) a) The congruence ~~k~~ $ax \equiv 1 \mod b$ has a sol'n x since $\gcd(a,b)=1$. Let $u = ax$. Then clearly $u \equiv 0 \mod a$ and $u \equiv 1 \mod b$.

Let $v = 1-u$. Then $v \equiv 1-0 \equiv 1 \mod a$ and $v \equiv 1-1 \equiv 0 \mod b$.

b) Let $x = \cancel{c \cdot u + d \cdot v}$ $c \cdot v + d \cdot u$. Then

$$x \equiv c \cdot 1 + d \cdot 0 \equiv c \mod a$$

and $x \equiv c \cdot 0 + d \cdot 1 \equiv d \mod b$,

as desired.

c) We must have $n = 16 + 17k$ for some k. The number k must be chosen so that

$$\begin{aligned}&16 + 17k \equiv 4 \mod 19\\ \iff\ &17k \equiv -12 \mod 19\\ \iff\ &-2k \equiv -12 \mod 19\\ \iff\ &k \equiv 6 \mod 19 \quad (\gcd(-2,19)=1).\end{aligned}$$

So let

$$\begin{aligned} n &= 16 + 6\cdot 1\cancel{9}7 \\ &= 16 + 102 \\ &= \cancel{130}.\ \boxed{118}. \end{aligned}$$

(4) We are given that $(a^m+1) \mid (a^n+1)$. ie.

$$a^n+1 \equiv 0 \bmod (a^m+1).$$

For convenience let $M = a^m+1$. Observe that $a^m \equiv -1 \bmod M$. Therefore, writing

$$n = q\cdot m + r \qquad (\text{for } r = n\%m),$$

it follows that

$$\begin{aligned} a^n+1 &\equiv (a^m)^q\cdot a^r + 1 \bmod M \\ &\equiv (-1)^q\, a^r + 1 \bmod M \end{aligned}$$

Now, since $a^n+1 \equiv 0 \bmod M$, we know that

$$a^r \equiv (-1)^{q+1} \bmod M.$$

Since $0 \le r < m$, we know that $1 \le a^r \le a^{m-1}$, ~~and $a^{m-1} \le a^m - 2$ since~~ therefore we must have that either $a^r = 1$

or $a^r = a^m - 1$.

In the first case, $r=0$, so $m \mid n$ as desired. In the second case, r must also be 0 or else a divides both a^r & a^m; hence $a|1$, which is impossible. So in either case, $r=0$ and $m|n$, as desired.

(5) 43 is prime, so by Fermat's little Theorem,

$$19^{5085} \equiv 19^{5085 \% 42} \bmod 43$$

Now, $5085 = 121 \cdot 42 + 3$, so

$$\begin{aligned} 19^{5085} &\equiv 19^3 \bmod 43. \\ &\equiv (19^2)\cdot 19 \equiv 361 \cdot 19 \bmod 43 \\ &\equiv 17 \cdot 19 \equiv 323 \\ &\equiv \boxed{22 \bmod 43} \end{aligned}$$

(6) We wish to find an exponent f s.t. $(x^{17})^f \equiv x \bmod 43$.
It suffices to solve

$$17f \equiv 1 \bmod 42.$$

Using the extended Euclidean algorithm:

$$\begin{aligned} [8] &= (42) - 2\cdot(17) \\ [1] &= (17) - 2\cdot[8] \\ &= (17) - 2(42) + 4(17) \\ &= 5(17) - 2(42) \end{aligned}$$

So let $f=5$.

$$\begin{aligned} & x^{17} \equiv 5 \bmod 43 \\ \Leftrightarrow\ & x^{17\cdot 5} \equiv 5^5 \bmod 43 \\ \Leftrightarrow\ & x \equiv 5^5 \bmod 43. \end{aligned}$$

Now, $5^2 \equiv 25$

$5^3 \equiv 125 \equiv -4$

$5^4 \equiv -20$

$5^5 \equiv -100 \equiv \underline{29}$ So $\boxed{x \equiv 29 \bmod 43}$