18) a) $p-1=52=2^2\cdot 13$. Thus calculate powers with exponent $\frac{p-1}{q}$ where q are primes:

$2^4 \equiv 16 \equiv 1 \pmod{53}$
$2^{26} \equiv 52 \not\equiv 1 \pmod{53}$
} The Order$\mathrm{Mod}_{53}(2)$ does not divide 4 or 26 $\Rightarrow$ Order is 52 $\Rightarrow$ 2 is prim. root.

b) Exhaustive search is the only method we know. Try out: $2, 2^2, \dots$ 2^{17} works.

19) a) $(a^k)^n \equiv (a^n)^k \equiv 1^k \pmod p \Rightarrow \mathrm{OrderMod}_p(a^k)$ must divide n

b): Assume $n=k\cdot m$. Then $(a^k)^m \equiv a^n \equiv 1 \pmod p$

Thus $O_k \mid m$. If the order was smaller, i.e. $(a^k)^e \equiv 1 \pmod p$ with $e<m$ then $1 \equiv (a^k)^e \equiv a^{ke} \pmod p$, but $1 \leq k\cdot e < km = n$ ↯ to order of a being n.

$\Rightarrow O_k = m = n/k$.

c) If $l = uk + vn$ then $(a^k)^u \equiv (a^k)^u \cdot 1 \equiv (a^k)^u (a^n)^v$

$\equiv a^{uk+vn} \equiv a^1 \pmod p$. Thus a is a power of a^k, thus n divides O_k (by a). As also $O_k | n \Rightarrow O_k = n$.

d) Let $b = a^{\gcd(n,k)}$. Let $d = \mathrm{OrderMod}_p(b)$. By b) we know that $d = \frac{n}{\gcd(n,k)}$. But if we write

$k = \gcd(n,k) \cdot m$, with $\gcd(d,m) = 1$ (otherwise the gcd would be larger) then $a = b^m$ with

$\gcd(m,d) = 1$. Thus by c) $O_k = d = \frac{n}{\gcd(n,k)}$

e) Let a be a primitive root, i.e. $n = p-1$. Then for a^k being a prim. root as well we must have that $\mathrm{OrdMod}_p(a^k) = n$, by d) this means that

$1 = \gcd(k,n) = \gcd(k, p-1)$

But there are exactly $q(p-1)$ such k.

20) We have $1001 = 7 \cdot 11 \cdot 13$. Assuming no kind of topping has more than 50 choices this means that there are 3 classes of toppings, each has 7, 11, respectively 13 choices (one choice might be not to take the topping).

21) Version d requires no multiplication and will never produce intermediate numbers that are larger than needed. (use dynamical programming to save on recursion cost.)