Pollard's $p-1$ Factoring Algorithm

As a quick review, Pollard's $p-1$ factoring algorithm is efficient only in the case where one of the primes, say p, has the property that $p-1$ is a product of small primes (such a $p-1$ is called a ***smooth number***). As a review, the specification of the algorithm in your textbook is as follows[1]:

Algorithm 1: Our text's version of ***Pollard's*** $p-1$ ***Algorithm***

input : N to be factored, and a bound B.
output: d, a non-trivial factor of N or ***failure***.

```
a ← 2
j ← 2
while j ≤ B do
    a ← a^j (mod N)
    d ← gcd(a − 1, N)
    if 1 < d < N then
        return d
    end if
    j ← j + 1
end while
return failure
```

As an example, let's factor the value $N = 6994241$ using Pollard's $p-1$ algorithm:

j	a	$a^j \pmod{N}$	d	Comments
2	2	4	1	
3	4	64	1	
4	64	2788734	1	
5	2788734	3834705	1	
6	3834705	513770	1	
7	513770	443653	3361	Return 3361

Dividing, we find that $6994241 = 3361 \cdot 2081$. Further investigating, we find that $3361 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7$, which is a 7-smooth number (that is, contains no prime factors larger than 7).

As a hint on your homework, using this algorithm for problem 3.21, you will need to proceed to $j = 6$ for part (a), $j = 8$ for part (b), and $j = 19$ for part (c).

[1] Please note: This is not a standard variation of this algorithm, so you aren't likely to be able to refer to other sources for examples or clarification.