**Notes on Pollard's $p-1$ Attack on RSA**

Let $n = pq$ be an RSA key where $p, q$ are primes. Pollard's attack is a method to find the factorization of $n$. The method will work (with a choice of a large integer $B$) provided:

- $p-1$ divides $B!$
- $q-1$ has a prime factor $> B$.

**Step 1:** Let $a = 2$ and compute $b \equiv a^{B!} \pmod{n}$.

**Step 2:** Calculate $\gcd(b-1,\, n)$. This should give the prime factor $p$.

**Step 3:** If $p$ is not found in step 2 repeat steps 1,2 with $a = 3$. If $a = 3$ fails keep trying other values for $a$.

Why does this work? Pollard's attack works because of Fermat's Little Theorem.

In fact, since $(p-1) \mid B!$ this implies that $B! = k \cdot (p-1)$ for some integer $k$. Recall that $b \equiv 2^{B!} \pmod{pq}$. It follows that

$$b \equiv 2^{B!} \pmod{p} \equiv 2^{k\cdot(p-1)} \equiv 1 \pmod{p}.$$

Hence $p$ divides $b-1$.

**Warning:** The method will work only if $b > 1$.

It will certainly be the case that $b > 1$ if 2 is a primitive root $\pmod{q}$, since we assumed that $\phi(q) = q-1$ has a prime factor $> B$, which implies $2^{B!} \not\equiv 1 \pmod{q}$.

If $a = 2$ doesn't work then try $a = 3$, etc, until a good choice of $a$ is obtained. Eventually the factorization of $n$ will be found.

**EXAMPLE:** Factor $n = 2573$ with Pollard's attack and $B = 5$..

**Step 1:** $B! = 5! = 120 = 64 + 32 + 16 + 8 = 2^6 + 2^5 + 2^4 + 2^3$.

$$\begin{aligned}
2^{2^1} \pmod{2573} &\equiv 4 \\
2^{2^2} \pmod{2573} &\equiv 16 \\
2^{2^3} \pmod{2573} &\equiv 256 \\
2^{2^4} \pmod{2573} &\equiv 1211 \\
2^{2^5} \pmod{2573} &\equiv 2484 \\
2^{2^6} \pmod{2573} &\equiv 202
\end{aligned}$$

$$\begin{aligned}
b \equiv 2^{120} \pmod{2573} &\equiv 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^4} \cdot 2^{2^3} \pmod{2573} \\
&\equiv 202 \cdot 2484 \cdot 1211 \cdot 256 \pmod{2573} \\
&\equiv 280
\end{aligned}$$

**Step 2:** $\gcd(279,\ 2573) = 31$. $\boxed{n = 31 \cdot 83.}$