(Lucas' Theorem) Let n be a positive integer. If there is a positive integer x such that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime factors q of $n-1$, then n is prime.

EXAMPLE 10.11 Using Lucas' theorem, show that $n = 1117$ is a prime.

SOLUTION

We shall choose $x = 2$ to show that n satisfies the conditions of the test.

First, notice that

$$\begin{aligned} 2^{1116} &= (2^{100})^{11} \cdot 2^{16} \\ &\equiv 293^{11} \cdot 750 \equiv 70 \cdot 750 \equiv 1 \pmod{1117} \end{aligned}$$

Since $1116 = 2^2 \cdot 3^2 \cdot 31$, the prime factors of $n - 1 = 1116$ are 2, 3, and 31.

When $q = 2$,

$$\begin{aligned} 2^{(n-1)/q} &= 2^{558} = (2^{50})^{11} \cdot 2^8 \\ &\equiv 69^{11} \cdot 256 \equiv 1069 \cdot 256 \equiv -1 \pmod{1117}; \end{aligned}$$

when $q = 3$,

$$\begin{aligned} 2^{(n-1)/q} &= 2^{372} = (2^{50})^7 \cdot 2^{22} \\ &\equiv 69^7 \cdot 1086 \equiv 112 \cdot 1086 \equiv 996 \pmod{1117}; \end{aligned}$$

when $q = 31$,

$$
\begin{aligned}
2^{(n-1)/q} &= 2^{36} = (2^{10})^3 \cdot 2^6 \\
&\equiv (-93)^3 \cdot 64 \equiv 1000 \cdot 64 \equiv 331 \pmod{1117}
\end{aligned}
$$

Thus, $2^{1116/q} \not\equiv 1 \pmod{1117}$ for all prime factors q of 1116. Therefore, by Lucas' theorem, 1117 is a prime. ■