giving that

$$24^2 \equiv -24 \pmod{100}.$$

Hence

$$24^4 \equiv (-24)^2 \pmod{100} \equiv 24^2 \pmod{100} \equiv -24 \pmod{100}.$$

Similarly,

$$24^8 \equiv -24 \pmod{100}, \quad 24^{16} \equiv -24 \pmod{100}, \quad 24^{32} \equiv -24 \pmod{100}.$$

Since $2^{20} \equiv -24 \pmod{100}$, it follows that

$$\begin{aligned} 2^{1000} &\equiv 2^{20 \cdot 50} \pmod{100} \equiv (-24)^{50} \pmod{100} \equiv 24^{50} \pmod{100} \\ &\equiv 24^{32} \cdot 24^{16} \cdot 24^2 \pmod{100} \equiv -24 \cdot -24 \cdot -24 \pmod{100} \\ &\equiv -24\left(24^2\right) \pmod{100} \equiv -24 \cdot -24 \pmod{100} \equiv 24^2 \pmod{100} \\ &\equiv -24 \pmod{100} \equiv 76 \pmod{100}. \end{aligned}$$

(2) Suppose we wish to prove that $97 \mid 2^{48} - 1$.

This is equivalent to showing that $2^{48} \equiv 1 \pmod{97}$. Indeed, we have that

$$\begin{aligned} & 2^6 = 64 \equiv -33 \pmod{97}, \\ \Rightarrow\ & 2^{12} \equiv (-33)^2 \pmod{97} \equiv 33^2 \pmod{97} \equiv 9 \cdot 121 \pmod{97} \equiv 9 \cdot 24 \pmod{97} \\ & \equiv 108 \cdot 2 \pmod{97} \equiv 11 \cdot 2 \pmod{97} \equiv 22 \pmod{97}, \\ \Rightarrow\ & 2^{24} \equiv 22^2 \pmod{97} \equiv 4 \cdot 121 \pmod{97} \equiv 4 \cdot 24 \pmod{97} \equiv 96 \pmod{97} \\ & \equiv -1 \pmod{97}, \\ \Rightarrow\ & 2^{48} \equiv (-1)^2 \pmod{97} \equiv 1 \pmod{97}. \end{aligned}$$

Theorem 12.13. *Let $x, y \in \mathbb{Z}$ and $\lambda, n, n_1, n_2, \ldots, n_r \in \mathbb{N}$. We have that*

(i) $\lambda x \equiv \lambda y \pmod{n} \Leftrightarrow x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$, *where* $d = (\lambda, n)$;

(ii) *if* $\lambda x \equiv \lambda y \pmod{n}$ *and* $(\lambda, n) = 1$, *then* $x \equiv y \pmod{n}$;

(iii) $x \equiv y \pmod{n_i}\ \forall i \in \{1, 2, \ldots, r\} \Leftrightarrow x \equiv y \pmod{[n_1, n_2, \ldots, n_r]}$.

Proof (i) Suppose that $\lambda x \equiv \lambda y \pmod{n}$. Then $n \mid \lambda x - \lambda y$, and hence $\exists k \in \mathbb{Z}$ such that $\lambda x - \lambda y = kn$. It follows that $\frac{\lambda}{d}(x - y) = k\frac{n}{d}$. Hence $\frac{n}{d} \mid \frac{\lambda}{d}(x - y)$.

Furthermore $(\lambda, n) = d$, and hence Corollary 10.10 gives that $\left(\frac{\lambda}{d}, \frac{n}{d}\right) = 1$. It follows from Corollary 10.12 that $\frac{n}{d} \mid x - y$. Hence $x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$.

Conversely, suppose that $x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$. Then $\frac{n}{d} \mid x - y$, and hence $\exists k \in \mathbb{Z}$ such that $x - y = k\frac{n}{d}$. Hence $\lambda x - \lambda y = \left(k\frac{\lambda}{d}\right) n$. It follows that $\lambda x \equiv \lambda y \pmod{n}$.