Označme $d=(x,y,m)$. Pro lib. prvočíslo p značí ν_p p-adický exponent. Symbol $p^r \| m$ značí $p^r \mid m$, $p^{r+1} \nmid m$.

Číslo $m \in \mathbb{N}$ rozložíme na součin tří po dvou nesoudělných čísel: $m = m_1 \cdot m_2 \cdot m_3$, přitom do m_3 přispějí prvočísla $p \mid m$ splňující

$$\min\{\nu_p(x), \nu_p(y)\} \geq \nu_p(m).$$

Do m_2 ostatní splňující navíc $\nu_p(y) > \nu_p(x)$. Konečně do m_1 ta zbylá.

Čínská zbytková věta dá $a \in \mathbb{Z}$, $a \equiv 0 \pmod{m_1}$, $a \equiv 1 \pmod{m_2}$

Protože $d \mid x, d \mid y$, existuje $v \in \mathbb{Z}$, že $ax+y = d \cdot v$.

Čínská zbytková věta dá $u \in \mathbb{Z}$ tak, že

$$u \equiv v \pmod{m_1 m_2}, \quad u \equiv 1 \pmod{m_3}$$

Pak

$$du \equiv dv = ax+y \pmod{m_1 m_2},$$
$$du \equiv 0 \equiv ax+y \pmod{m_3},$$

a tedy $du \equiv ax+y \pmod{m}$. Ukážeme, že $(u,m)=1$.

1) $p \mid m_1 \Rightarrow \nu_p(dv) = \nu_p(ax+y) = \nu_p(y)$, neboť $\nu_p(y) < \nu_p(a)$,
tedy $\nu_p(dv) = \nu_p(y) = \nu_p(d)$, odtud $p \nmid v$, tj. $p \nmid u$

2) $p \mid m_2 \Rightarrow \nu_p(dv) = \nu_p(ax+y) = \nu_p(x)$, neboť $\nu_p(ax) = \nu_p(x) < \nu_p(y)$,
tedy $\nu_p(dv) = \nu_p(x) = \nu_p(d)$, odtud $p \nmid v$, tj. $p \nmid u$

3) $p \mid m_3 \Rightarrow p \nmid u$ z definice.