Problem for 2017 February

Proposed by Dan Jurca

a. Suppose p is a prime number, n is a positive integer, x is a positive integer, and

$$x \equiv a \pmod{p^n}$$

where $0 < a < p^n$. Show that there exists a positive integer y such that

$$xy \equiv a \pmod{p^{n+1}} \text{ and } \gcd(p, y) = 1.$$

b. Suppose a and b are integers, $2 \leq a$, $2 \leq b$, and $\gcd(a, b) = 1$. Show that there exists a positive integer x such that

$$x \equiv a \pmod{ab},$$

but there does not exist an integer y such that

$$xy \equiv a \pmod{a^2 b}.$$

Solution by the proposer

We recall that if a and b are positive integers and $\gcd(a, b) = 1$, then there exist (non-unique) integers u and v such that $ua + vb = 1$, and we remark that by subtracting and adding a suitable multiple of ab, one may assume that $v < 0$. (In fact if $n < -v/a$, then $na + v < 0$ and $ua - nab + nab + vb = (u - nb)a + (na + v)b = 1$.)

Now if $p,\ a,\ x$, and n are as in a., then there exists a positive integer b such that $x = a + bp^n$. There exist integers m and c such that $0 \leq m < n,\ 0 < c,\ a = p^m c$ and $\gcd(c, p) = 1$; and (by the division theorem) there exist (unique) integers q and r such that $b = pq + r,\ 0 \leq r < p$. Suppose $uc + vp = 1$ and $u < 0$. Let $y = -rup^{n-m} + 1$. Then $0 < y$ and $\gcd(p, y) = 1$. We show that $xy \equiv a \pmod{p^{n+1}}$.

$$\begin{aligned}
xy &= (a + bp^n)(-rup^{n-m} + 1) \\
&= -arup^{n-m} + a - brup^{2n-m} + bp^n \\
&= a - p^m c \cdot rup^{n-m} - brup^{2n-m} + (pq + r)p^n \\
&= a - r \cdot (uc) \cdot p^n - brup^{2n-m} + qp^{n+1} + rp^n \\
&= a - r \cdot (1 - vp) \cdot p^n - brup^{2n-m} + qp^{n+1} + rp^n \\
&= a - rp^n + rvp^{n+1} - brup^{n-m-1+n+1} + qp^{n+1} + rp^n \\
&= a + (rv - brup^{n-m-1} + q)p^{n+1},
\end{aligned}$$

and since $0 \leq m < n,\ 0 < n - m$, so $0 \leq n - m - 1$, and $xy \equiv a \pmod{p^{n+1}}$.

Now suppose $2 \leq a,\ 2 \leq b$, and $\gcd(a, b) = 1$. Suppose u and v are integers, $ua + vb = 1$, and $v < 0$, and let $x = a + (-v)ab$. Then x is a positive integer and $x \equiv a \pmod{ab}$. We show there does not exist an integer y such that $xy \equiv a \pmod{a^2 b}$. For

$$\begin{aligned}
xy &= (a - vab)y \\
&= ay - vaby \\
&= ay - a \cdot vb \cdot y \\
&= ay - a(1 - ua)y \\
&= ay - ay + a^2 uy \\
&= a^2 uy, \quad \text{and if} \\
xy &= a + qa^2 b \text{ for some integer } q, \text{ then} \\
a^2 uy &= a + qa^2 b, \text{ whence} \\
auy &= 1 + qab,
\end{aligned}$$

so that $(uy - qb)a = 1$, which contradicts the given $2 \leq a$.

Remark. Because of b. one exercises care in generalizing a. to moduli other than prime powers.