# 1. \( x^2 \equiv 1 \mod p \) iff \( p \) divides \( x^2 - 1 = (x+1)(x-1) \) iff \( p \mid (x+1) \) or \( p \mid (x-1) \) by Euclid’s Lemma. iff \( x \equiv 1 \mod p \) or \( x \equiv -1 \mod p \) iff \( x \equiv \pm 1 \mod p \).

# 2. (a) 24 = \[3 \times 7 + 8\]
(b) \(-24 = -4 \times 7 + 4\)
(c) \(7 = 0 \times 24 + 7\)
(d) \(10^{24} = 10^{17} \times 10^7 + 0\)
(e) \(10^{24} = (10^{17} + 10^3) \times (10^3 - 1) + 10^3 - 1\)

# 3. \[
\begin{array}{c|c|c|c}
45321 & 4321 & 1 & 0 \\
654321 & 4321 & 1 & 0 \\
1850 & 621 & 151 & -1 \\
608 & 13 & 303 & 2 \\
13 & 1 & 1060 & 329 \\
10 & 3 & 50577 & -334 \\
1 & 1 & 201248 & 1329 \\
\end{array}
\]

Check: \(1329 \times 654321 - 201248 \times 4321 = 1\).

# 4. \( 456 x = 789 \mod 123 \) iff \( 87x = 51 \mod 123 \) iff \( 87x = 51 + 123k \) for some \( k \in \mathbb{Z} \) iff \( 29x = 17 + 41k \) for some \( k \in \mathbb{Z} \) iff \( 29x \equiv 17 \mod 41 \) iff \( x \equiv 17 \times 17 = 289 \equiv 2 \mod 41 \).

The solution set is \( \{ x \in \mathbb{Z} : x \equiv 2 \mod 41 \} \)
\[= \{ \ldots, -80, -39, 2, 43, 84, \ldots \} \]
5. (a) F (b) F (c) F (d) T (e) F (f) T (g) F (h) T (i) F (j) F

Comments:
6 divides 0, but 6 \not\div 0 and 16 \not\div 101. This is a counterexample to both (a) and (b).

(d) If \( b = ra \) and \( a = sb \) for some \( r, s \in \mathbb{Z} \) then \( b = rsb \), i.e. \( (rs-1)b = 0 \). Either \( r = s = \pm 1 \) (in which case \( a = \pm b \) as required) or \( b = 0 \) (in which case also \( a = 0 \) so once again \( a = \pm b \) follows).

(e) A counterexample is given by \( 2 \mid -2 \), \(-2 \mid 2 \) but \( 2 \not\mid -2 \).

(h) A counterexample is given by \( 1 \mid 2 \), \( 2 \mid 2 \) but \( 3 \nmid 4 \).

(f) \( d \mid a \) iff \( a = kd \) for some \( k \in \mathbb{Z} \)
   iff \( (-a) = (-k)d \) for some \( k \in \mathbb{Z} \)
   iff \( d \mid (-a) \).

(g) If \( b = ra \) and \( d = sc \) for some \( r, s \in \mathbb{Z} \), then
   \( bd = (rs)(ac) \) so \( ac \mid bd \).

(h) This is trivially true. (If \( a^2 \equiv 1 \pmod{n} \) then
   \( a^2 \equiv 1 \) or \( a^2 \equiv -1 \pmod{n} \). This follows from the meaning of \( \equiv \) without any consideration of congruences necessary.) The intended statement was "If \( a^2 \equiv 1 \pmod{n} \) then necessarily \( a^2 \equiv 1 \pmod{n} \)" which is false, as the example \( a = 3, n = 8 \) shows.

(i) Consider the counterexample \( 4 \mid 12, 6 \mid 12 \) but \( 24 \nmid 12 \).

(j) Consider the counterexample \( 4 \mid 2 \cdot 6 \) but \( 4 \nmid 2, 4 \nmid 6 \).