Proof (of Presburger's theorem):

Consider formula $\exists x : \mathcal{C}(x, \bar{y})$,

where $\mathcal{C}(x, \bar{y})$ is quantifier-free.

Step 1: Normalize formula

↳ Transform $\mathcal{C}(x, \bar{y})$ into negation normal form (NNF), where negation only applies to atomic propositions.

↳ Eliminate negation:

$$\neg(t_1 = t_2) \quad \text{iff} \quad t_1 < t_2 \vee t_2 < t_1$$
$$\neg(t_1 < t_2) \quad \text{iff} \quad t_1 = t_2 \vee t_2 < t_1$$
$$\neg(t_1 \equiv_m t_2) \quad \text{iff} \quad t_1 \equiv_m t_2 + 1 \vee t_1 \equiv_m t_2 + 2 \vee \ldots \vee t_1 \equiv_m t_2 + (m-1)$$

↳ Compute DNF of the resulting formula:

$\exists x : \gamma_1 \vee \ldots \vee \gamma_n$ where γ_i = conjunction of atomic formulas.

$\equiv \exists x : \gamma_1 \vee \ldots \vee \exists x : \gamma_n$.

From now on, focus on a single $\exists x\, \gamma$

↳ Let $\exists x : \gamma = \exists x : \alpha_1 \wedge \ldots \wedge \alpha_n$ where each α_i is atomic.

↳ Wlog. assume x occurs in each α_i, and each α_i has one of the following forms

$$nx + t = u$$
$$nx + t \equiv_m u$$
$$nx + t < u$$
$$u < nx + t,$$

where $n \geq 1$ and u, t terms (that may be 0) that do not contain x.

As in the construction of Presburger automata, add subtraction and write

$$nx = u - t$$
$$nx \equiv_m u - t$$
$$nx < u - t$$
$$u - t < nx$$

(Shortcuts for the formulas where the terms are on the correct side)

Step 2: Uniformize and eliminate coefficients on x:

↳ We have

$$\exists x: \alpha_1 \wedge \dots \wedge \alpha_n$$

with coefficients $n_1, \dots, n_n$ on x

↳ Compute

$$p := \operatorname{lcm}(n_1, \dots, n_n).$$ → least common multiple

↳ Transform each α_i so that coefficient of x is p:

$$nx = u - t$$

iff $\frac{p}{n} \cdot nx = \frac{p}{n} u - \frac{p}{n} t$ → integer since $n \mid p$.

For modulo:

$$nx \equiv_m u - t$$

iff $\frac{p}{n} \cdot nx \equiv_{(\frac{p}{n} \cdot m)} \frac{p}{n} u - \frac{p}{n} t$

↳ Replace px by new variable y and add $y \equiv_p 0$:

$$px = u' - t'$$

is replaced by

$$y = u' - t'$$
$$\wedge\ y \equiv_p 0.$$

Intuition:

Instead of $\exists x : 5x = \dots$

we say $\exists y : y = \dots \wedge y \equiv_5 0.$

"There is a multiple of 5, named y, that satisfies ..."

Altogether, this transforms

$\exists x : \alpha_1 \wedge \dots \wedge \alpha_n$ into $\exists y : \alpha_1' \wedge \dots \wedge \alpha_n' \wedge \alpha_{n+1}'$

Step 3.a: Special case: There is $= on y$

↳ Assume some α_i' is

$$y = u' - t'.$$

↳ Transform all α_j':

$$\alpha_j'' := \alpha_j' \{ u' - t' / y \}$$

↳ Replace α_i' by

$$t' \leq u'.$$

↳ This already eliminates y.

Step 3.b: There is no $= on y$:

Now

$$\exists y : \alpha_1' \wedge \dots \wedge \alpha_n' \wedge \alpha_{n+1}'$$

is of the form

$$\exists y : \Big(\bigwedge_{i=1}^{\ell} r_i' - s_i' < y \Big) \wedge \Big(\bigwedge_{i=1}^{k} y < t_i' - u_i' \Big) \wedge \Big(\bigwedge_{i=1}^{n} y \equiv_{m_i} v_i' - w_i' \Big)$$

→ Lower bounds

→ Upper bounds.

where $r_i', s_i', t_i', u_i', v_i', w_i'$ are terms without y.

Case 3.6.1: There are no congruences

Then the formula requires the following:

"there is a distance of at least two between lower and upper bound"

Replace formula by

$$\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{l} (r_j' - s_j') + 1 < t_i' - u_i' \wedge \bigwedge_{i=1}^{k} 0 < t_i' - u_i'$$

Case 3.6.2: There are congruences

↳ Compute

$$M = \mathrm{lcm}(m_1', \ldots, m_n')$$

↳ This M satisfies

$$a + M \equiv_{m_i'} a$$

for all $a \in \mathbb{N}$ and all $m_i' \in \{m_1', \ldots, m_n'\}$.

↳ This means the remainders modulo all m_i' have a recurring pattern with period M:

Example:

Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13 ..
$\equiv_2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\equiv_3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1

↳ Assume now there is a natural number y

- that satisfies lower bounds $L_1, \ldots, L_e$,
- that satisfies upper bounds,
- and that satisfies the congruences.

↳ To satisfy upper bounds, choose small y

↳ To satisfy congruences, go through $0, \dots, M-1$.

Hence, if there is a solution,
one of the following will be a solution:

$$\begin{array}{l} L_1, \; L_1+1, \dots, \; L_1+M-1 \\ L_2, \; L_2+1, \dots, \; L_2+M-1 \\ \vdots \\ L_\ell, \; L_\ell+1, \dots, \; L_\ell+M-1 \\ 0, \; 1, \dots, \; M-1. \end{array}$$

Last row for the case that all L_j negative.
To avoid case distinctions, add lower bound

$$r'_{\ell+1} - s_{\ell+1} < y \quad \text{with} \quad r'_{\ell+1} = 0 \text{ and } s_{\ell+1} = 1$$

Now we can replace the $\exists$-quantified formula

$$\exists y : \alpha'_1 \wedge \dots \wedge \alpha'_\ell \wedge \alpha_{\ell+1}$$

by

$$\bigvee_{j=1}^{\ell+1} \bigvee_{q=0}^{M-1} \Bigg[\bigwedge_{i=1}^{\ell+1} r_i' - s_i' < \underbrace{(r_j' - s_j') + q}_{\text{for } y} \wedge \bigwedge_{i=1}^{k} (r_j' - s_j') + q < t_i' - u_i' \wedge \bigwedge_{i=1}^{n} (r_j' - s_j') + q \equiv_{m_i} v_i' - w_i' \Bigg].$$

Examples:

1.) $\exists y: (1 < y \wedge y < 100 \wedge y \equiv_2 1 \wedge y \equiv_3 2)$

↳ b is required form

↳ Coefficients 1

↳ There is no $= c_n y$

↳ There are congruences

Case 3.b.2:

· Compute

$$M := \operatorname{lcm}(2,3) = 6$$

· Replace $\exists$-quantified formula S_y

$$\bigvee_{q=0}^{5} (1 < 1+q \wedge 1+q < 100 \wedge 1+q \equiv_2 1 \wedge 1+q \equiv_3 2)$$

$\underline{q = 4}$

$$1 < 5 \wedge 5 < 100 \wedge 5 \equiv_2 1 \wedge 5 \equiv_3 2$$

2.) $\exists x: (w < 4x \wedge 2x < u \wedge 3x < v \wedge x \equiv_3 t)$

where w, u, v, t terms without x.

↳ b is the required form

Step 2: Uniformize and eliminate coefficients:

· Compute $\rho := \operatorname{lcm}(4,2,3) = 12$

· $\exists x: (\frac{12}{4} w < \frac{12}{4} 4x \wedge \frac{12}{2} 2x < \frac{12}{2} u \wedge \frac{12}{3} 3x < \frac{12}{3} v \wedge \frac{12}{1} x \equiv_{\frac{12}{1}\cdot 3} \frac{12}{1} t$

$= \exists x: (3w < 12x \wedge 12x < 6u \wedge 12x < 4v \wedge 12x \equiv_{36} 12t)$

Replace $12x$ by variable y:

$$\exists y : (3u < y \wedge y < 6u \wedge y < 4v \wedge y \equiv_{36} 12t \wedge y \equiv_{12} 0)$$

↳ There is no $=$ on y

Case 3.6.2: There are congruences:

- Compute
$$M := \operatorname{lcm}(36, 12) = 36.$$
- Add lower bound
$$\exists y : (3w < y \wedge 0 - 1 < y \wedge y < 6u \wedge y < 4v \wedge y \equiv_{36} 12t \wedge y \equiv_{12} 0)$$
- Replace quantifier on y:

$$\bigvee_{q=0}^{35} (3w < 3w + q \wedge 0 - 1 < 3w + q \wedge 3w + q < 6u \wedge 3w + q < 4v \wedge 3w + q \equiv_{36} 12t \wedge 3w + q \equiv_{12} 0)$$

$$\vee \bigvee_{q=0}^{35} (3w < (0-1) + q \wedge 0 - 1 < (0-1) + q \wedge (0-1) + q < 6u \wedge (0-1) + q < 4v \wedge (0-1) + q \equiv_{36} 12t \wedge (0-1) + q \equiv_{12} 0)$$