Examples of Diophantine relations:

1. $a \equiv b \pmod c$: $\exists x\colon a = cx + b$ or $b = cx + a$. (over $\mathbb{N}$!)
2. $a \geq b$: $a = b + x$ ($\exists$ is always implicit)
3. $a > b$: (Exercise)
4. $a = b \bmod c$: $a \equiv b \pmod c$ and $0 \leq a < c$.
5. $\{ (a, b, c) \mid a = b^c \}$? **Exponentiation is Diophantine!**
6. $\{ 2^k \}$? Tarski believed not Diophantine

$G_b(0) = 0$, $G_b(1) = 1$, $\boxed{\begin{array}{l} G_b(n+1) = b \cdot G_b(n) - G_b(n-1) \\ G_b(n-1) + G_n(n+1) = b \cdot G_b(n) \end{array}}$ close to the recursion for b^{n-1}
$\rightleftarrows$ symmetric between forward and backward

$b = 4$: $[\ldots, -15, -4, -1,]\, 0, 1, 4, 15, 56, \ldots$
$b = 3$: $0, 1, 3, 8, 21, \ldots$
$b = 2$: $0, 1, 2, 3, 4, 5, \ldots$ (useless?)

WE SHOW: $\boxed{a = G_b(c)}$ for (fixed) $b \geq 3$ is Diophantine. ($b \geq 4$ simplifies some arguments.)
Missing link! [Yuri Matiyasevich 1970, Julia Robinson, Martin Davis, Hilary Putnam 1961]

The points $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} G_b(n+1) \\ G_b(n) \end{pmatrix}$ lie on the hyperbola $\boxed{h_b(x, y) := x^2 - bxy + y^2 - 1 = 0}$. ($\to$ picture)

Lemma 1. *The only integer solutions of $h_b(x, y) = 0$ with $x > y \geq 0$ are those points.*

Proof: The hyberbola is invariant under the shift $\binom{G_b(n)}{G_b(n-1)} \leftrightarrow \binom{G_b(n+1)}{G_b(n)}$: $\binom{x}{y} \mapsto \binom{bx-y}{x}$ or $\binom{x}{y} \mapsto \binom{y}{by-x}$, and the shift preserves $y < x$. $\square$

Now we can generate $\{ G_b(n) \} = \{ x \mid \exists y\colon h_b(x, y) = 0 \}$ but we don't know n.

Lemma 2. $b \equiv b' \pmod u \implies G_b(n) \equiv G_{b'}(n) \pmod u$ (Induction. Easy.) $\square$

IDEA: Choose two appropriate moduli M and m to coordinate $G_b(n)$ with n:
$G_w(0), G_w(1), \ldots, G_w(n), \ldots \bmod M$ $\quad w \equiv b \pmod M$ $\quad \boxed{\to G_b(n)}$
$G_w(0), G_w(1), \ldots, G_w(n), \ldots \bmod m$ $\quad w \equiv 2 \pmod m$ $\quad \boxed{\to G_2(n) = n}$

As long as n is small and $G_w(n) \leq M$, we have $G_w(n) \bmod M = G_b(n)$ (and $G_w(n) \bmod m = n$), but for larger n, $G_w(n) \bmod M$ gets out of control, and there will be extra solutions. ($\to$ picture)

- Make $G_w(n) \bmod M$ mirror-symmetric after reaching a peak at $G_w(p) = G_b(p)$: ($\to$ picture)
  $G_b(p-1) \equiv G_b(p+1) \pmod M \implies M := G_b(p+1) - G_b(p-1)$ (p = peak = period)
- Avoid "negative" values by using the absmod operation instead of mod. ($\to$ picture)
  $x \operatorname{absmod} M = a \iff x = qM \pm a$ and $0 \leq a \leq M/2$.
- The period m of "$G_w(n) \operatorname{absmod} m = n$" should divide the period $2p$ of "$G_w(n) \operatorname{absmod} M$": $m \mid p$.
- Choose m (and M) larger than twice the (supposed) value a of $G_b(c)$, so that absmod does no harm.

1. $m > 2a$
2. p should be a multiple of m
3. $M := G_b(p+1) - G_b(p-1)$
4. Choose $w > 2$ with $w \equiv b \pmod M$
   $w \equiv 2 \pmod m$
5. $h_w(x, y) = 0$ [$\implies x = G_w(n)$ for some n]
6. $a = x \operatorname{absmod} M$ $\quad$ [$a = G_b(n)$]
   $c = x \operatorname{absmod} m$ $\quad$ [$c = G_2(n) = n$]

Lemma 3. $G_b(k)^2 \mid G_b(p) \implies G_b(k) \mid p$ $\square$

Also: $G_b(k) \mid G_b(p) \iff k \mid p$ (Cf. Fibonacci numbers: $F_k \mid F_p \iff k \mid p$.)

Application: Choose m of the form $m = G_b(k)$ for some k, by requiring $\boxed{h_b(m, m') = 0}$.
Then $m^2 \mid G_b(p) \implies m \mid p$.

Implementation of Conditions 2 and 3.

$\boxed{h_b(r, s) = 0,\ r < s}$ $\quad \begin{aligned} G_b(p-1) &= r, \text{ for some } p \\ G_b(p) &= s \\ G_b(p+1) &= bs - r \end{aligned}$

$\boxed{M = (bs - r) - r}$ $[= G_b(p+1) - G_b(p-1).$ Also $G_b(p) < M/2.$ $]$

$\boxed{m^2 \mid s}$ $[\implies m \mid p.$ $]$

The conditions are enough to ensure that every solution (a, c) satisfies $a = G_b(c)$. (The condition $a < m/2$ cuts off extra solutions.)

Converse direction:
We need to show that m, M with $\gcd(m, M) = 1$ exist (then w statisfying (4.) exists, by the Chinese Remainder Theorem), and that $m^2 \mid s$ can be fulfilled.

- Choose $m = G_b(k)$ odd and set $s = G_b(p)$ for $p = k \cdot m$:

  Then it can be shown that $\gcd(m, M) = 1$ and $m^2 \mid s$.

Getting to the relation $a = b^c$:

$$(b-1)^n \leq G_b(n+1) \leq b^n$$

$$b^c = \lim_{x \to \infty} \frac{G_{bx+4}(c+1)}{G_x(c+1)} \approx \frac{(bx \pm \text{const})^c}{(x \pm \text{const})^c} \to b^c, \text{ for all } b, c \geq 0$$

The "+4" term ensures that this works even for $b = 0$.

$$b^c = \left\lfloor \frac{G_{bx+4}(c+1)}{G_x(c+1)} \right\rfloor \quad \text{for } x > 16(c+1)G_{b+4}(c+1).$$