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

\[
\begin{align*}
G_b(0) &= 0, \quad G_b(1) = 1, \\
G_b(n+1) &= b \cdot G_b(n) - G_b(n-1), \\
G_b(n+1) + G_n(n+1) &= b \cdot G_b(n)
\end{align*}
\]

\( b = 4: \ldots, 15, -4, -1, 0, 1, 4, 15, 56, \ldots \)

\( b = 3: \) 0, 1, 3, 8, 21, \ldots

\( b = 2: \) 0, 1, 2, 3, 4, 5, \ldots (useless?)

**WE SHOW:** \( a = G_b(c) \) \( \) for \( (\text{fixed}) b \geq 3 \) is Diophantine. \( \) \( (b \geq 4 \) simplifies some arguments.\)


The points \( \left( \frac{x_n}{y_n} \right) = \left( \frac{G_b(n+1)}{G_b(n)} \right) \) lie on the hyperbola \( h_b(x, y) := x^2 - bxy + y^2 - 1 = 0 \). (\( \rightarrow \) picture)

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

Proof: The hyperbola is invariant under the shift \( \left( G_b(n) \right) \leftrightarrow \left( G_b(n+1) \right): \left( \frac{x}{y} \right) \rightarrow \left( \frac{bx-y}{x} \right) \) or \( \left( \frac{x}{y} \right) \rightarrow \left( \frac{y-x}{by} \right) \), and the shift preserves \( y < x \).

Now we can generate \( \{ G_b(n) \} = \{ x | \exists y: h_b(x, y) = 0 \} \) 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.)

IDEA: Choose two appropriate moduli \( M \) and \( m \) to coordinate \( G_b(n) \) with \( n \):

\[
\begin{align*}
G_w(0), G_w(1), \ldots, G_w(n), \ldots \pmod{M} & \quad w \equiv b \pmod{M} & \rightarrow G_b(n) \\
G_w(0), G_w(1), \ldots, G_w(n), \ldots \pmod{m} & \quad w \equiv 2 \pmod{m} & \rightarrow G_2(n) = n
\end{align*}
\]

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

- Make \( G_w(n) \pmod{M} \) mirror-symmetric after reaching a peak at \( G_w(p) = G_b(p) \): (\( \rightarrow \) 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. (\( \rightarrow \) picture)
  \( x \text{ absmod } M = a \iff x = qM \pm a \) and \( 0 \leq a \leq M/2 \).

- The period \( m \) of \( \text{“} G_w(n) \text{ absmod } m = n \text{”} \) should divide the period \( 2p \) of \( \text{“} G_w(n) \text{ absmod } M \text{”} : m | p \).

- 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 \( w \equiv b \pmod{M} \)
5. \( h_w(x, y) = 0 \] \( \implies x = G_w(n) \) for some \( n \)
6. \( a = x \text{ absmod } M \) \( \] \( a = G_b(n) \] \( \]
   \( c = x \text{ absmod } m \) \( \] \( c = G_2(n) = n \)
Lemma 3. $G_b(k)^2 \mid G_b(p) \implies G_b(k) \mid p$

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 $h_b(m, m') = 0$.
Then $m^2 \mid G_b(p) \implies m \mid p$.

Implementation of Conditions 2 and 3.

\[
\begin{align*}
\h_b(r, s) = 0, \ r < s & \quad G_b(p - 1) = r, \text{ for some } p \\
G_b(p) & = s \\
G_b(p + 1) & = bs - r \\
M = (bs - r) - r & = G_b(p + 1) - G_b(p - 1). \text{ Also } G_b(p) < M/2. \\
m^2 \mid s & \implies m \mid p.
\end{align*}
\]

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 $w$ satisfying (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 $b = 0$.

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