Warmup.

Once upon a time, you had to do this type of problems:

Example 1 (1990 AIME Q15 / Probably some SMO Round 1)
Find $ax^5 + by^5$ if the real numbers a, b, x, and y satisfy the equations

$$\begin{aligned} ax + by &= 3, \\ ax^2 + by^2 &= 7, \\ ax^3 + by^3 &= 16, \\ ax^4 + by^4 &= 42. \end{aligned}$$

1 Understanding Recurrences

A *linear recurrence* is an infinite sequence $\{x_n\}$ that satisfies

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + ... + a_0x_n$$

for all integers $n \geq 0$ and some coefficients a_i. I'm sure you've seen these pop up in various places by now.

Perhaps the only way you were taught to understand linear recurrence was via the general formula (if you forgot what it is, it's provided as a theorem later on). But that's such a shame, because there are so many (other) exciting ways to understand them[1], which are purely conceptual: no calculations involved!

2 Recap: the main fact

To jog your memory:

Fact (General Formula for Linear Recurrences)
Suppose $\{x_i\}$ is a sequence satisfying

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + ... + a_0x_n$$

forll integers $n \geq 0$. Then x_n has the following general formula:

$$x_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + ... + P_m(n)\alpha_m^n$$

where the α_i are the roots of the **characteristic polynomial**:

$$x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_0 = (x - \alpha_1)^{\beta_1}(x - \alpha_2)^{\beta_2}...(x - \alpha_m)^{\beta_m}$$

and P_i are polynomials with degree at most β_i.

Wooooooooooah hold up. This is complicated, and you shouldn't memorize it wholesale. You can remember this by two important cases:

Example 2 (Distinct roots case)
If the characteristic polynomial has distinct roots (i.e. $\beta_i = 1$ for all i), then all the P_i are forced to be constants:

$$x_n = P_1 \cdot \alpha_1^n + P_2 \cdot \alpha_2^n + ... + P_m \cdot \alpha_k^n$$

[1] and in some sense, this will be your first (indirect) exposure to linear algebra

Example 3 (Finite Differences)

If the characteristic polynomial is $(x-1)^k$, then x_n is simply a degree k polynomial in n.

In particular, the recurrence relationship can be phrased in the following way. For a sequence $\{x_n\}$, define the sequence $\{\Delta x_n\} = \{x_{n+1} - x_n\}$ [a]. In particular, we can iterate Δ's:

$$\{\Delta^2 x_n\} = \{\Delta(\Delta x)_n\} = \{x_{n+2} - 2x_{n+1} + x_n\}$$

and so on. It isn't hard to check that having the characteristic polynomial be $(x-1)^k$ is the same as saying $\Delta^k x_n = 0$ for all n.

[a] you should imagine the parantheses: it's actually $(\Delta x)_n$

2.1 Important tips and tricks

- You can capture the behavior of a "sum of exponents" function with a linear recurrence.
- Linearity is your best friend.
- Recurrence are sometimes related to combinatorial objects.

Problems

1. (HMMT 2017 Team Q8) Show that for any prime p, there exists irrational $\alpha > 1$ such that $\lfloor \alpha^n \rfloor$ is a multiple of p for all $n \geq 1$.

Solution. Let $\alpha > \beta$ be the roots of $x^2 - (1000p+1)x + p = 0$, and check that both roots are positive with $\beta < 1$. Set $a_n = \alpha^n + \beta^n$, then $a_0 = 2, a_1 = 1000p + 1$ and inductively $a_n \equiv 1 \pmod{p}$. But $0 < \alpha^{-n} < 1$, so $p \mid a_n - 1 = \lfloor \alpha^n \rfloor$.

2. (ELMO 2017/6) Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that for all real numbers a, b, and c:

(i) If $a + b + c \geq 0$ then $f(a^3) + f(b^3) + f(c^3) \geq 3f(abc)$.

(ii) If $a + b + c \leq 0$ then $f(a^3) + f(b^3) + f(c^3) \leq 3f(abc)$.

Solution. Start off with

$$(0,0,0) : f(0) = 0$$
$$(a, a-\varepsilon), 0 : f \text{ is non-decreasing}$$
$$(a^{1/3}, -a^{1/3}, 0) : f(-a) = -f(a)$$

Now we do a trick: plug $(a^{1/3}, a^{1/3}, -2a^{1/3})$ to get

$$2f(a) - f(8a) = 3f(2a)$$

This means that if $a_k = f(2^k a)$, then a_k satisfies a linear recurrence (with characteristic functions having roots $2, -1, -1$), so

$$a_k = c_1 \cdot 2^k + c_2 \cdot (-1)^k + c_3 \cdot k(-1)^k$$

This really can't satisfy non-decreasing-ness: by taking $k \to -\infty$ (yes we can extend the recurrence relation backwards), we conclude that $c_2 = c_3 = 0$, so $f(2x) = 2f(x)$ for all x.

We can repeat the argument with $(a^{1/3}, (n-1)a^{1/3}, -na^{1/3})$ to get

$$((n-1)^3 + 1)f(a) - f(n^3 a) = 3(n-1)f(na)$$

with the roots of the characteristic equation being $\left(n, \frac{-n \pm (n-2)\sqrt{-3}}{2}\right)$. Once again, the other coefficients must be 0, so in general $f(nx) = nf(x)$. Then we are done, since it's linear on the rationals and non-decreasing.

3. (China TST 2020 Q1) Let ω be a primitive n-th root of unity. Given complex numbers $a_1, a_2, \cdots, a_n$ of which $p > 0$ are non-zero, define $\{b_k\}_{1 \leq k \leq n}$ by

$$b_k = \sum_{i=1}^{n} a_i \omega^{ki}.$$

Prove that at least $\frac{n}{p}$ numbers in $b_1, b_2, \cdots, b_n$ are non-zero.

Solution. Verify that $a_k = \frac{1}{n} \sum_{j=1}^{n} b_k \omega^{-jk}$. Since p of them are nonzero, we can write

$$b_k = \sum_{j=1}^{p} a_{i_j} \omega^{i_j k}$$

therefore $\{b_k\}$ is a linearly recurrent relation of degree at most p. In particular, if p consecutive values are 0, then all b_k are zero and so all a_k are zero, which is a contradiction. So no p consecutive values of b_k are zero (i.e. at least n/p values are nonzero).

Remark. In this problem, $\{b_k\}$ is in fact the *discrete Fourier transform* of $\{a_k\}$. The formula for $\{a_k\}$ in terms of $\{b_k\}$ is precisely an analogue of the Fourier inversion formula.

Alternative Solution. (jouzch, on AoPS) Let

$$A = \{j : a_j \neq 0\}, \qquad B = \{j : b_j \neq 0\}$$

It's well-known that $|b_1|^2 + \cdots + |b_n|^2 = n(|a_1|^2 + \cdots + |a_n|^2)$, i.e.

$$\sum_{j\in B} |b_j|^2 = n(\sum_{j\in A} |a_j|^2)$$

Since $|b_j| \leq \sum_{j\in A} |a_j|$, apply Cauchy-Schwarz on the RHS above to get $|B| \geq \frac{n}{|A|} = \frac{n}{p}$.

Remarks. The well-known statement above is the discrete analogue of Plancherel's formula.

4. (Putnam Diagnostic Test) Let $a_1, a_2, ..., a_n$ be fixed positive integers. Find all functions $f : \mathbb{Z} \to \mathbb{R}$ where

$$\sum_{i=1}^{n} f(k + a_i\ell) = 0$$

for all $k, \ell \in \mathbb{Z}$, $\ell \neq 0$.

Solution. By setting $\ell = 1$, the sequence $\{f(n)\}$ corresponds to a degree $M = \max\{a_i\}$ linear recurrence with characteristic polynomial

$$P(x) = \sum_{i=1}^{n} x^{M-a_i}$$

So $\{f(n)\}$ satisfies a recurrence relation. But the strange fact is that $\{f(an + b)\}$ also satisfies the recurrence relation!

In particular, suppose the solution is of the form

$$f(k) = \sum_{i=1}^{m} Q_i(k)\alpha_i^k$$

By considering $\{f(\ell k)\}$, α_i^k must be a root of $P(x)$. Hence the set $\{\alpha_i^k\}$ is finite, so all α_i's are roots of unity.

This means that f is periodic, and setting ℓ to be the period we find that $f \equiv 0$.

5. (IDMO 2 Q5) Let $c_1, c_2, \ldots, c_k$ be integers. Consider sequences $\{a_n\}$ of integers satisfying

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$$

for all $n \geqslant k + 1$. Prove that there is a choice of initial terms $a_1, a_2, \ldots, a_k$ not all zero satisfying: there is an integer b such that p divides $a_p - b$ for all primes p.

Solution (Official, talkon)**.** If $c_1, c_2, \ldots, c_k$ are all zero, choose $a_i = k!$ for all $i = 1, 2, \ldots, k$. The recurrence relation gives us $a_n = 0$ for all $n \geqslant k + 1$. Not hard to see that this gives $p \mid a_p \implies a_p \equiv 0 \pmod{p}$ for all primes p.

Now, suppose $c_1, c_2, \ldots, c_k$ are not all zero. Let $z_1, z_2, \ldots, z_k$ be the roots (counting multiplicities) of the characteristic equation $\lambda^k - \sum_{i=1}^{k} c_i\lambda^{k-i} = 0$. The key part is choosing

$$a_n = z_1^n + z_2^n + \cdots + z_k^n$$

for all n.

By Vieta, we get that the elementary symmetric polynomials

$$e_j = \sum_{1\leq i_1<i_2<\ldots<i_j\leq k} z_{i_1}z_{i_2}\ldots z_{i_j} = (-1)^{j+1}c_j$$

is an integer for all $j = 1, 2, \ldots, k$. By the Fundamental Theorem of Symmetric Polynomials, we get that $P(z_1, z_2, \ldots, z_k)$ is an integer for all symmetric polynomials $P \in \mathbb{Z}[x_1, x_2, \ldots, x_k]$. In particular, a_n is an integer for all $n \in \mathbb{Z}^+$.

To prove that $a_1, a_2, ..., a_k$ are not all zero, note that if $a_i = 0$ for all $i = 1, 2, \ldots, k$, we can use

Newton's identities to prove by induction on i that $\sigma_i = 0$ for all $i = 1, 2, \ldots, k$. This implies $c_i = 0$ for all $i = 1, 2, \ldots, k$, which is a contradiction.

Now, for each prime p, we've

$$c_1^p = (z_1 + z_2 + ... + z_k)^p = \sum_{i=1}^{k} z_i^p + pT(z_1, z_2, ..., z_k) = a_p + pT(z_1, z_2, ..., z_k)$$

for some symmetric polynomial $T \in \mathbb{Z}[x_1, x_2, ..., x_k]$. So, $T(z_1, z_2, ..., z_k)$ is an integer. This gives $a_p \equiv c_1^p \equiv c_1 \pmod{p}$, so we are done by choosing $b = c_1$.

6. (Kvant) Suppose that 2^n consecutive integers each belong to at least one of n given arithmetic progressions. Show that all integers belong to at least one of those arithmetic progressions.

Solution. Suppose the n APs are $\{a_i + kd_i\}$ for $i = 1, 2, ..., n$. Consider

$$z_n = \prod_{i=1}^{n} \left((1 - \exp\left(\frac{2\pi i(n - a_i)}{d_i} \right) \right)$$

which detects if n is among any of the APs. By hypothesis, this is 0 for 2^n consecutive values. However, we can also expand this to obtain

$$z_n = \sum_{m=1}^{2^n} a_j \zeta_j^m$$

for some $a_j, \zeta_j \in \mathbb{C}$. So $\{z_n\}$ satisfies a nontrivial recurrence of degree at most 2^n, so it is the 0-sequence. But this means all of $\mathbb{Z}$ is covered.

Remark. This can also be used to nail down this problem:

(Stronger version of ELMO 2013/3) Let $m_1, \ldots, m_{2013} > 1$ be 2013 pairwise relatively prime positive integers and $A_1, \ldots, A_{2013}$ be 2013 sets with $A_i \subseteq \{1, \ldots, m_i - 1\}$ for all i. Prove that there is a positive integer N such that

$$N \leq (|A_1| + 1) \cdots (|A_{2013}| + 1)$$

and for each i, there does not exist $a \in A_i$ such that m_i divides $N - a$.

7. (CMO 2017 Q1) The sequences $\{u_n\}$ and $\{v_n\}$ are defined by $u_0 = u_1 = 1$,$u_n = 2u_{n-1} - 3u_{n-2}$ $(n \geq 2)$, $v_0 = a, v_1 = b, v_2 = c$,$v_n = v_{n-1} - 3v_{n-2} + 27v_{n-3}$ $(n \geq 3)$. There exists a positive integer N such that when $n > N$, we have $u_n \mid v_n$. Prove that $3a = 2b + c$.

Solution. The key is to realise what connects the two given recurrence relations.

Note that if α, β are the roots of $x^2 - 2x + 3 = 0$, then $\alpha^2, \beta^2, \alpha\beta = 3$ are the roots of $x^3 - x^2 + 3x - 27 = 0$. Hence, for any two sequences $\{a_n\}, \{b_n\}$ satisfying the recurrence relation of $\{u_n\}$, then $\{a_n b_n\}$ must satisfy the recurrence relation of v_n.

Hence in particular, we wish to define $\{w_n\}$, satisfying the same recurrence relation as $\{u_n\}$, such that $\{v_n - (u_n \cdot w_n)\}$ (which still satisfies the recurrence relation of v_n) has its 3^n term isolated. Now we balance the coefficients: let the first three terms be $\lambda, 3\lambda, 9\lambda$, thus the first three terms of $\{w_n\}$ are $a - \lambda, b - 3\lambda, 9\lambda - c$, and checking the original relation we get $9\lambda - c = 2(b - 3\lambda) - 3(a - \lambda)$, or $\lambda = \frac{2b+c-3a}{12}$.

Since v_n are integers for all sufficiently large n, a, b, c must be rational, so the first two terms of w_n are rational too, so let $k \in \mathbb{N}$ be such that kw_n are all integers. then $u_n | k\lambda \cdot 3^n$ for all sufficiently large n, but u_n is unbounded and not divisible by 3, so $\lambda = 0$.

B. Suppose the sequence of integers $\{x_n\}$ satisfy a linear recurrence (with real coefficients). Must it satisfy a linear recurrence of the form

$$x_{n+k} = a_{k-1} x_{n+k-1} + ... + a_0 x_n$$

where a_i are integers?

Solution (Fatou's lemma)**.** The answer (shockingly) is **yes**. Suppose the original recurrence satisfies suck a recurrence relation with $a_i \in \mathbb{R}$.

(1): First we show that we can get $a_i \in \mathbb{Q}$. Pick some large $N > k$, the consider the following system of equations:

$$\begin{aligned} a_0x_1 + ... + a_{k-1}x_k &= x_{k+1} \\ a_0x_2 + ... + a_{k-1}x_{k+1} &= x_{k+2} \\ &... \\ a_0x_N + ... + a_{k-1}x_{N+k-1} &= x_{N+k} \end{aligned}$$

There is a solution $(a_0, ..., a_{k-1}) \in \mathbb{R}^k$. Pick $C > \max_{1 \le i \le N+k-1}\{x_i\}$. Then, by standard Diophantine arguments we get that there exists integer M such that $\|Ma_i\|_{\mathbb{R}/\mathbb{Z}} < 1/(kC)$, where $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ is just fancy notation for the distance away from the nearest integer.

If we now set a_i' to be the nearest multiple of $1/M$ from a_i, we can easily check that $(a_0', ..., a_{k-1}') \in \mathbb{Q}^k$ is also a solution.

So $y_n = a_0'x_n + ... + a_{k-1}'x_{n+k-1} - x_{n+k}$ is 0 for N consecutive values but also satisfies the original deg $k < N$ recurrence relation. Hence, $\{y_n\}$ is the 0-sequence, and we may WLOG let the recurrence instead be

$$x_{n+k} = a_{k-1}'x_{n+k-1} + ... + a_0'x_n$$

(2): Now we show that they must all be integers. This has a very "Gauss Lemma"-esque flavor to it. [tbcf]

Remark. It could have been coefficients in $\mathbb{C}$, but we could have just taken the real/imaginary parts separately.