NON-STANDARD TECHNIQUES APPEARED IN PUTNAM

GYUJIN OH

In principle, all Putnam problems have solutions understandable for those who know materials from high school level comptetitive mathematics plus lower level undergraduate mathematics such as calculus, linear algebra, group theory and complex analysis. However, some Putnam problems are not very accessible, in a sense that one cannot easily reach the solution without a priori getting used to a specific fact. In other words, a clever solution of a Putnam problem to a stranger might be standard to a more knowledgeable person. Here I summarize the occasions of such problems. I write this primarily for myself, so please excuse any errors. Also, this note is not meant to be self-contained by the same reason.

1. Discrete Fourier Analysis (or Representation Theory)

Even though the subject has a scary name of discrete fourier analysis, it is really just about getting information of the original group by considering the duals, or the characters (You don't necessarily need to know what the original Fourier analysis is). To be more precise, for a finite cyclic group G, we consider a character, $f : G \to \mathbb{C}^\times$. Originally, the term of discrete Fourier analysis came from the idea of lifting discrete sums to a circle and performing Fourier transform. As the representation theory of finite group gives the "full" information on the group, and since all irreducible representations of G are 1-dimensional, it is sufficient to only consider characters, not any other higher dimensional analogues. The same applies for the group of characters, and the interplay between the original group and the character group is very similar to that of Fourier transform. The similar reasoning applies to any abelian group, thereby giving the name of discrete fourier analysis on abelian group.

For the rest of this section, let G be a finite abelian group. Let $\widehat{G}$ be the group of characters of G. From the representation theory of finite groups, we have orthogonality relations, namely

$$(\chi, \psi) := \frac{1}{|G|} \sum_{a \in G} \overline{\chi(a)} \psi(a) = \begin{cases} 1 & \text{if } \chi = \psi \\ 0 & \text{otherwise} \end{cases},$$

for any characters ψ, χ of G, and

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \chi(b) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise} \end{cases},$$

for any $a, b \in G$. By dimensional reason, $\widehat{G}$ is an orthonormal basis of $\mathbb{C}^G$, the set of functions $f : G \to \mathbb{C}$. Thus, given $f : G \to \mathbb{C}$, we can write it uniquely as a linear combination of characters,

$$f = \sum_{\chi \in \widehat{G}} c_\chi \chi,$$

which is some sort of *Fourier series*. We define the *Fourier transform* $\widehat{f} : \widehat{G} \to \mathbb{C}$ of f as

$$\widehat{f}(\chi) = \sum_{a \in G} \chi(a) f(a) = |G| c_{\overline{\chi}}.$$

This process is obviously invertible. We can define an inner product on $\mathbb{C}^{\widehat{G}}$ as

$$(f, g) := \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{f(\chi)} g(\chi).$$

We expect discrete analogues of some basic things in Fourier analysis, such as:

$$\widehat{\delta_a}(\chi) = \chi(a),$$

where δ_a is the indicator function of $a \in G$; the Plancherel formula,

$$(\widehat{f}, \widehat{g}) = |G|(f, g),$$

for $f, g \in \mathbb{C}^G$;

$$(\chi_A, \chi_B) = \frac{1}{|G|} |A \cap B|,$$

for characteristic functions χ_A, χ_B of $A, B \subset G$; and last but not least, the compatibility with convolution product! We define the convolution

$$(f * g)(a) := \frac{1}{|G|} \sum_{b \in G} f(ab^{-1}) g(b),$$

for $f, g \in \mathbb{C}^G$, then as in the original picture, it is associative, and we have

$$\widehat{(f * g)}(\chi) = \widehat{f}(\chi) \widehat{g}(\chi).$$

These are all just identities about finite sums, so nothing is really fancy. This is more like a generalization of the trick using roots of unity and generating functions, for counting something with pattern modulo some number. This point of view turns out to be very crucial in understanding some problems. For example:

Problem (2011 A6). Let G be an abelian group with n elements, and let

$$\{g_1 = e, g_2, \cdots, g_k\} \subset G$$

be a (not necessarily minimal) set of distinct generators of G, strictly smaller than G. A special die, which randomly selects one of the elements $g_1, \cdots, g_k$ with equal probability, is rolled m times and the selected elements are multiplied to produce an element $g \in G$. Prove that there is a real number $b \in (0, 1)$ such that

$$\lim_{m \to \infty} \frac{1}{b^{2m}} \sum_{x \in G} \left(\text{Prob}(g = x) - \frac{1}{n} \right)^2$$

is positive and finite.

Remark. To understand why the discrete Fourier analysis is a generalization of root of unity trick, try the above problem in the case of $G = \mathbb{Z}/n\mathbb{Z}$, $k = 2$, $g_2 = \zeta_n$.

Proof. I would rather write the group multiplication additively.

Discrete Fourier analysis is extremely useful in counting the number of solutions of an equation of form $g_1 + g_2 + \cdots + g_m = 0$ exactly in terms of character values. For example, given subsets $A_1, \cdots, A_m \subset G$, consider the problem of counting solutions of $g_1 + \cdots + g_m = 0$, with restrictions that $g_i \in A_i$ for each i. Surprisingly, the number of solutions has an explicit expression in terms of character values. Namely, it is

$$\frac{1}{|G|} \sum_{\psi \in \widehat{G}} \prod_{i=1}^{m} \widehat{\chi_{A_i}}(\psi).$$

Why?? It is because the number of solutions is

$$\sum_{g_i \in A_i} \delta_0(g_1 + \cdots + g_m),$$

which is equal to

$$\begin{aligned}
\sum_{g_i \in A_i} \delta_0(g_1 + \cdots + g_m) &= \frac{1}{|G|} \sum_{g_i \in A_i} \sum_{\psi \in \widehat{G}} \psi(g_1 + \cdots + g_m) \\
&= \frac{1}{|G|} \sum_{\psi \in \widehat{G}} \sum_{g_i \in A_i} \prod_{i=1}^{m} \psi(g_i) \\
&= \frac{1}{|G|} \sum_{\psi \in \widehat{G}} (\chi_{A_1} * \cdots * \chi_{A_m})^{\wedge}(\psi) \\
&= \frac{1}{|G|} \sum_{\psi \in \widehat{G}} \prod_{i=1}^{m} \widehat{\chi_{A_i}}(\psi).
\end{aligned}$$

Now we apply this to our problem. Let A be the designated set of generators. Then, $\mathrm{Prob}(g = x)$ is $\frac{1}{k^m}$ times the number of solutions of $a_1 + \cdots + a_m = x$ with restriction that $a_i \in A$, which is equal to

$$\frac{1}{nk^m} \sum_{\psi \in \widehat{G}} \widehat{\chi_A}(\psi)^{m-1} \widehat{\chi_{A-x}}(\psi).$$

Note that the sum for $\psi = 1$ gives k^m, so

$$\mathrm{Prob}(g = x) - \frac{1}{n} = \frac{1}{nk^m} \sum_{\psi \in \widehat{G} - \{1\}} \widehat{\chi_A}(\psi)^{m-1} \widehat{\chi_{A-x}}(\psi).$$

Expanding, we have

$$\begin{aligned}
\mathrm{Prob}(g = x) - \frac{1}{n} &= \frac{1}{nk^m} \sum_{\psi \in \widehat{G} - \{1\}} (\psi(g_1) + \cdots + \psi(g_k))^{m-1} (\psi(g_1 - x) + \cdots + \psi(g_k - x)) \\
&= \frac{1}{nk^m} \sum_{\psi \in \widehat{G} - \{1\}} (\psi(g_1) + \cdots + \psi(g_k))^{m} \psi^{-1}(x),
\end{aligned}$$

and

$$\sum_{x\in G}\left(\text{Prob}(g=x)-\frac{1}{n}\right)^2 = \frac{1}{n^2k^{2m}}\sum_{\psi,\psi'\in\widehat{G}-\{1\}}(\psi(g_1)+\cdots+\psi(g_k))^m(\psi'(g_1)+\cdots+\psi'(g_k))^m \cdot\sum_{x\in G}\psi^{-1}(x)\psi'^{-1}(x).$$

Note that the last sum is nonzero only if $\psi'=\psi^{-1}$. Thus,

$$\begin{aligned}\sum_{x\in G}\left(\text{Prob}(g=x)-\frac{1}{n}\right)^2 &= \frac{1}{nk^{2m}}\sum_{\psi\in\widehat{G}-\{1\}}(\psi(g_1)+\cdots+\psi(g_k))^m(\overline{\psi(g_1)}+\cdots+\overline{\psi'(g_k)})^m\\ &= \frac{1}{n}\sum_{\psi\in\widehat{G}-\{1\}}\left(\frac{|\psi(g_1)+\cdots+\psi(g_k)|}{k}\right)^{2m}.\end{aligned}$$

For any $\psi\in\widehat{G}-\{1\}$, $|\psi(g_1)+\cdots+\psi(g_k)|<k$, as $\psi(g_i)$'s are roots of unity, $\psi(g_1)=1$ and not all $\psi(g_i)$'s are 1 as $\psi\neq 1$ and g_i's generate G. Thus, taking

$$b=\frac{\max_{\psi\in\widehat{G}-1\{1\}}|\psi(g_1)+\cdots+\psi(g_k)|}{k},$$

we are done (i.e. the limit is $\frac{1}{n}$ times the number of $\psi\in\widehat{G}-\{1\}$ reaching the maximum value of $|\psi(g_1)+\cdots+\psi(g_k)|$) if we show that $b>0$. If $b=0$, then this means that $\psi(g_1)+\cdots+\psi(g_k)=0$ for all $\psi\neq 1$. Then,

$$\sum_{\psi\in\widehat{G}}\sum_{i=1}^{k}\psi(g_i)=k.$$

As g_i's are distinct, $g_i\neq 1$ unless $i=1$. Thus

$$\sum_{i=1}^{k}\sum_{\psi\in\widehat{G}}\psi(g_i)=n.$$

This implies that $n=k$, contradicting with the fact that A is a proper subset of G. □

Yet another take....

Problem (2013 A6). Define a function $w:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ as follows. For $|a|,|b|\le 2$, let $w(a,b)$ be as in the table shown; otherwise, let $w(a,b)=0$.

	$w(a,b)$	$b=-2$	-1	0	1	2
	-2	-1	-2	2	-2	-1
	-1	-2	4	-4	4	-2
a	0	2	-4	12	-4	2
	1	-2	4	-4	4	-2
	2	-1	-2	2	-2	-1

For every finite subset S of $\mathbb{Z} \times \mathbb{Z}$, define

$$A(S) = \sum_{(\mathbf{s},\mathbf{s}') \in S \times S} w(\mathbf{s} - \mathbf{s}').$$

Prove that if S is any finite nonempty subset of $\mathbb{Z} \times \mathbb{Z}$, then $A(S) > 0$.

Proof. If we use the same notation of χ_S being the characteristic function of S, $A(S)$ can be expressed as

$$A(S) = \sum_{s,s' \in \mathbb{Z} \times \mathbb{Z}} w(s - s')\chi_S(s)\chi_S(s').$$

This is some form of convolution product, and we want to use some Fourier analysis on it. We can use the analogue for $\mathbb{Z} \times \mathbb{Z}$, but it is not immediate to justify the wellness of such theory (e.g. what is the Fourier transform on $\mathbb{Z} \times \mathbb{Z}$?). Instead, note that the sum is after all a finite sum. Thus, we can chop the whole picture at the boundary and pretend like we are working modulo N, for some big $N > 0$. Then we can use the discrete Fourier analysis for $G = (\mathbb{Z}/N\mathbb{Z})^2$. As both w and χ_S are elements of $\mathbb{C}^G$, we can Fourier expand them as $w = \sum_\psi c_\psi \psi$ and $\chi_S = \sum_\psi d_\psi \psi$. Then,

$$A(S) = \sum_{s,s' \in G} \sum_{\psi_1,\psi_2,\psi_3 \in \widehat{G}} c_{\psi_1} d_{\psi_2} d_{\psi_3} \psi_1(s - s')\psi_2(s)\psi_3(s').$$

But then by orthogonality, after switching the sums, the sum over s and s' would vanish unless $\psi_1\psi_2 = 1$ and $\psi_1^{-1}\psi_3 = 1$. Thus we get

$$A(S) = |G|^2 \sum_{\psi \in \widehat{G}} c_\psi d_\psi d_{\psi^{-1}}.$$

As χ_S is real-valued, $d_{\psi^{-1}} = d_{\overline{\psi}} = \overline{d_\psi}$, which implies that

$$A(S) = |G|^2 \sum_{\psi \in \widehat{G}} c_\psi |d_\psi|^2.$$

Therefore, it is sufficient to prove that $(\psi, w) = c_\psi > 0$ for every $\psi \in \widehat{G}$. As every $\psi \in \widehat{G}$ is of form $\psi(a, b) = \exp(2\pi(a\alpha + b\beta)/N) = \zeta_N^{a\alpha+b\beta}$ for some $\alpha, \beta \in \mathbb{Z}$, it is therefore sufficient to prove that

$$\begin{aligned}
&12 - 4(\zeta_N^{\alpha} + \zeta_N^{-\alpha} + \zeta_N^{\beta} + \zeta_N^{-\beta}) + 4(\zeta_N^{\alpha} + \zeta_N^{-\alpha})(\zeta_N^{\beta} + \zeta_N^{-\beta}) \\
&-2(\zeta_N^{2\alpha} + \zeta_N^{-2\alpha})(\zeta_N^{\beta} + \zeta_N^{-\beta}) - 2(\zeta_N^{\alpha} + \zeta_N^{-\alpha})(\zeta_N^{2\beta} + \zeta_N^{-2\beta}) \\
&+2(\zeta_N^{2\alpha} + \zeta_N^{-2\alpha} + \zeta_N^{2\beta} + \zeta_N^{-2\beta}) - (\zeta_N^{2\alpha} + \zeta_N^{-2\alpha})(\zeta_N^{2\beta} + \zeta_N^{-2\beta}) > 0.
\end{aligned}$$

Well, this seems to be a polynomial of $\cos(2\pi\alpha/N)$ and $\cos(2\pi\beta/N)$. Let those be denoted as x, y, respectively. Then the above inequality simplifies to

$$12 - 8(x + y) + 16xy - 8(2x^2 - 1)y - 8x(2y^2 - 1) + 4(2x^2 + 2y^2 - 2) - 4(2x^2 - 1)(2y^2 - 1) > 0,$$

or

$$xy - x^2y - xy^2 + x^2 + y^2 - x^2y^2 > 0,$$

or

$$x^2 + xy + y^2 > xy(xy + x + y),$$

or

$$(x+y)^2 > xy(x+1)(y+1).$$

This is just a hope; does this actually hold? No, but the one with $\geq$ instead of $>$ holds! If $xy \geq 0$, the inequality obviously holds, and for $xy > 0$,

$$(x+y)^2 \geq 4xy \geq (x+1)(y+1)xy.$$

The condition for the equality is $x = y = 0$ or $x = y = 1$. Thus, if $A(S) = 0$, then this means that $d_\psi \neq 0$ for $\psi \in \widehat{G}$ with two possibilities, either $\psi = 1$ or $\psi(a,b) = i^{\pm a \pm b}$. Then χ_S must be 4-periodic. However we can choose N to be so big that there is a big buffer of zeros outside S when cut out, which ensures χ_S not to be 4-periodic. Therefore, $A(S) > 0$. $\square$

Both problems have a common feature of counting solutions of form $a_1 + \cdots + a_k = m$ with restrictions on a_i's, and for such problems the idea of using some form of Fourier analysis (especially using convolution products) is crucial. I think it is hopeless to come up with any solutions of those two problems in a restricted amount of time without knowing this discrete Fourier analysis technique. Also 2015 A6 might heavily depend on discrete Fourier analysis by induction :)

2. Matrix Groups and Matrix Identities

Oddly, matrix itself is more cryptic than linear algebra. And you might not get even elementary facts about matrices themselves if you didn't think about them before.

There are elementary matrix identities which measures how much the inverse or the determinant would differ after a small perturbation. The most general identity I know is the binomial inverse theorem. If A, U, B, V are matrices of sizes $p \times p, p \times q, q \times q, q \times p$, respectively, then

$$(A+UBV)^{-1} = A^{-1} - A^{-1}UB(B+BVA^{-1}UB)^{-1}BVA^{-1},$$

provided that A and $B + BVA^{-1}UB$ are invertible. This is just a pure algebra. Even the whole verification is written in Wikipedia. However, this identity is surprisingly useful. Obviously no one can memorize this, and I think for Putnam this kind of generality is unnecessary after all. The two most useful variants are when B is the identity matrix and when U, V are the identity matrices. For the former case we have

$$(A+UV)^{-1} = A^{-1} - A^{-1}U(I_q + VA^{-1}U)^{-1}VA^{-1},$$

and for the latter case we have

$$(A+B)^{-1} = A^{-1} - A^{-1}B(B+BA^{-1}B)^{-1}BA^{-1}.$$

Actually the original identity can be derived from the first case by putting BV in it, and it is more memorizable (at least for me?).

Another way of deriving matrix identities is to use block matrices. When the dimensions are correctly divided, you can do the same matrix algebra for block matrices, and this yields many nontrivial identities. For example, $\det(I+AB) = \det(I+BA)$, for A, B of correct dimensions (precisely, A^T and B are of the same dimensions), can be seen directly from the following:

$$\begin{pmatrix} I & 0 \\ B & I \end{pmatrix} \begin{pmatrix} I+AB & A \\ 0 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ -B & I \end{pmatrix} = \begin{pmatrix} I & A \\ 0 & I+BA \end{pmatrix}.$$

And there are a lot of past Putnam problems where matrices are either perturbed by a specific matrix or treated as if they were entries of a bigger matrix. The examples are:

Problem (1999 B5). For an integer $n \geq 3$, let $\theta = 2\pi/n$. Evaluate the determinant of the $n \times n$ matrix $I + A$, where I is the $n \times n$ matrix and $A = (a_{jk})$ has entries $a_{jk} = \cos(j\theta + k\theta)$ for all j, k.

Proof. Identity + two rank 1 matrices! Easy. □

Problem (1992 B5). Let D_n denote the value of the $(n-1) \times (n-1)$ determinant

$$\begin{bmatrix} 3 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 4 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 5 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 6 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n+1 \end{bmatrix}.$$

Is the set $\{\frac{D_n}{n!}\}_{n \geq 2}$ bounded?

Proof. Diagonal + rank 1 matrix! Also easy. □

Problem (1987 B5). Let O_n be the n-dimensional zero vector. Let M be a $2n \times n$ matrix of complex numbers such that whenever $(z_1, \cdots, z_{2n})M = O_n$, with complex z_i, not all zero, then at least one of the z_i is not real. Prove that for arbitrary real numbers $r_1, \cdots, r_{2n}$, there are complex numbers $w_1, \cdots, w_n$ such that

$$\mathrm{Re}\left[M \begin{pmatrix} w_1 \\ \cdots \\ w_n \end{pmatrix} \right] = \begin{pmatrix} r_1 \\ \cdots \\ r_n \end{pmatrix}.$$

Proof. Treat the real and imaginary parts separately, and you can then construct block $2n \times 2n$ matrices. Then the problem becomes clear by considering the rank. □

Problem (1986 B6). Suppose A, B, C, D are $n \times n$ matrices with entries in a field F, satisfying the conditions that AB^T and CD^T are symmetric and $AD^T - BC^T = I$. Prove that $A^T D - C^T B = I$.

Proof. This is equivalent to $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ being a symplectic matrix. Namely, for $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, the condition of the problem is $MJM^T = J$. Taking the inverses of the both sides, as $J^{-1} = -J$, we get $J = (M^{-1})^T J M^{-1}$, or $M^T J M = J$. This gives $A^T D - C^T B = I$. This problem is also not a great choice for Putnam as this exact fact is very well known (called *Luneberg relations*). □

The above problems are immediate once you know the two techniques of block matrices and matrix identities. However, without knowing them it would be very hard to solve the above problems. For matrix identities I feel like one might manage to prove them in the contest without knowing them a priori, but for block matrices it's very difficult without prior knowledge. Especially for the latter two the block matrix method is almost implied by the problems, so if you haven't seen it before you would be in trouble when you face such problem in the contest.