PRIMES Math Problem Set: Solutions

Evan Chen

PRIMES 2019

Solution to General Math Problems

Problem G1

We flip a fair coin ten times, recording a 0 for tails and 1 for heads. In this way we obtain a binary string of length 10.

(a) Find the probability there is exactly one pair of consecutive equal digits.

(b) Find the probability there are exactly n pairs of consecutive equal digits, for every $n = 0, \dots, 9$.

Solution

The answer to (b) is $\frac{\binom{9}{n}}{2^9}$. To see this, by swapping the roles of heads and tails we may assume that the first flip is tails (without loss of generality). Thus there are 2^9 sequences. On the other hand, a sequence of heads and tails which starts with tails is uniquely determined by the choice for each $i = 1, \dots, 9$ of whether the ith flip and the $(i+1)$st flip are different or the same. Thus, if we would like n pairs to be the same, there are exactly $\binom{9}{n}$ such sequences.

Hence for (a) the answer is $\frac{9}{2^9}$.

Problem G2

For which positive integers p is there a nonzero real number t such that

$$t+\sqrt{p} \quad \text{and} \quad \frac{1}{t}+\sqrt{p}$$

are both rational?

Solution

The answer is that p must either be a square or one more than a perfect square.

If p is a perfect square, then $t=1$ works. If $p=k^2+1$ for some integer k, then $t=k-\sqrt{p}$ works, since $\frac{1}{t}=-(k+\sqrt{p})$.

Now assume p is not a square but such t exists. Let $t+\sqrt{p}=a$ and $1/t+\sqrt{p}=b$ for rational a and b, so that

$$1=(a-\sqrt{p})(b-\sqrt{p})=-(a+b)\sqrt{p}+(ab+p).$$

Since $\sqrt{p}$ is irrational, this can only happen if $a+b=0$. Then the above equation reads $1=p-a^2$, so $p=a^2+1$ (and clearly a has to be an integer).

Problem G3

Points A and B are two opposite vertices of a regular octahedron. An ant starts at point A and, every minute, walks randomly to a neighboring vertex.

(a) Find the expected (i.e. average) amount of time for the ant to reach vertex B.

(b) Compute the same expected value if the octahedron is replaced by a cube (where A and B are still opposite vertices).

Solution

For (a): we let x denote the expected value of the number of steps starting from A. Moreover, we let y denote the expected value of the number of steps starting from one of the four vertices other than A or B (these are equal by symmetry). Then we have

$$\begin{aligned} x &= y + 1 \\ y &= \frac{x + y + y + 0}{4} + 1. \end{aligned}$$

Solving we get $y = 5$ and $x = 6$. Hence the answer is 6 minutes.

For (b): let x denote the expected value starting from A, y the expected value starting from a neighbor of A, z the expected value starting from a neighbor of B. Then

$$\begin{aligned} x &= y + 1 \\ y &= \frac{x + z + z}{3} + 1 \\ z &= \frac{y + y + 0}{3} + 1. \end{aligned}$$

Solving gives $(x, y, z) = (10, 9, 7)$, so the answer is 10 minutes.

Problem G4

For a positive integer n, let $f(n)$ denote the smallest positive integer which neither divides n nor $n+1$.

(a) Find the smallest n for which $f(n) = 9$.

(b) Is there an n for which $f(n) = 2018$?

(c) Which values can $f(n)$ take as n varies?

Solution

For part (a), note that such an n should satisfy

$$\begin{aligned} n &\equiv -1 \text{ or } 0 \pmod 7 \\ n &\equiv -1 \text{ or } 0 \pmod 8. \end{aligned}$$

By the Chinese remainder theorem, we conclude

$$n \in \{-1, 0, 7, 7^2 - 1\} \equiv \{0, 7, 48, 55\} \pmod{56}.$$

Thus the first few candidates for n are $n \in \{0, 7, 48, 55, 56, 63, 104, 111, 112, 119, \dots\}$. We need an n such that $15 \mid n(n+1)$ and $9 \nmid n(n+1)$. A calculation then shows the value $n = 119$ works and is the smallest possible.

The answer to (b) is yes as $2018 = 2 \cdot 1009$ is twice a prime. This will be a corollary of part (c) to follow, but we comment that it suffices to pick n such that $n + 1 \equiv 0 \pmod{1009}$ and $n \equiv 0 \pmod r$ for any $1 < r < 2018$ with $r \neq 1009$.

As for (c), we claim $f(n)$ should be twice a prime or a prime power other than 2. These will be repeated applications of Chinese remainder theorem. To prove that these work:

- To get n such that $f(n) = 2p$ for p an odd prime, pick n such that $n \equiv 0 \pmod r$ for any number $1 < r < 2p$ and $r \neq p$, but $n + 1 \equiv 0 \pmod p$.
- To get n such that $f(n) = p^e$ for p a prime and $p^e \neq 2$, pick n such that $n \equiv 0 \pmod r$ for any $1 < r < p^e$ not divisible by p, but $n + 1 \equiv p^{e-1} \pmod{p^e}$.

Next, we claim that we never have $f(n) = ab$ if $\gcd(a, b) = 1$ and $\min(a, b) > 2$. The proof is by contradiction. Indeed, note that $2a$ and $2b$ are strictly less than $f(n)$, so $2a$ divides either n or $n+1$, similarly $2b$ divides either n or $n+1$. If n is even, then we find $2a$ and $2b$ both divide n, and since $\gcd(a, b) = 1$ we have $\operatorname{lcm}(2a, 2b) = 2ab$ divides n, contradiction. The case where $n + 1$ is even is exactly the same.

We now show (again by contradiction) we cannot have $f(n) = 2p^e$ for any odd prime p and $e \geq 2$. The numbers $2p$ and p^e are strictly less than $f(n)$, and so if p divides n (and hence not $n + 1$) we have $\operatorname{lcm}(2p, p^e) = 2p^e$ dividing n, contradiction. Again the case where p divides $n + 1$ instead is similar. This completes the proof.

Finally, it's easy to see $f(n) \neq 2$ for any n.

Problem G5

A pile with $n \geq 3$ stones is given. Two players Alice and Bob alternate taking stones, with Alice moving first. On a turn, if there are m stones left, a player loses if m is prime; otherwise he/she may pick a divisor $d \mid m$ such that $1 < d < m$ and remove d stones from the pile.

(a) Which player wins for $n = 6$, $n = 8$, $n = 10$?

(b) Determine the winning player for all n.

Solution

We claim that Alice wins if and only if n is even and $n \neq 2^{2k+1}$ for any $k \geq 0$. The proof is by (strong) induction on n.

We take the base case as those situations where n is prime, which clearly work (as $2 = 2^{2\cdot 0+1}$ and the rest of the primes are odd). The inductive step requires several cases:

- Suppose a player is faced with an odd number n. Then they must subtract an odd divisor d, so $n - d$ is even. Moreover, $n - d$ is divisible by d, so it is not a power of 2. Thus by induction hypothesis $n - d$ is winning for their opponent.
- Suppose a player is faced with $n = 2^{2k+1}$. Then they must subtract an even divisor d to get the even number $n - d$, which is not an odd power of 2 (it is a power of 2 only if $d = 2^{2k}$, but then $n - d = 2^{2k}$). Thus by induction hypothesis $n - d$ is winning for their opponent.
- Suppose on the other hand a player is faced with $n = 2^{2k}$. They may choose $d = 2^{2k-1}$ so $n - d = 2^{2k-1}$ is losing for their opponent by induction hypothesis.
- Finally, suppose a player is faced with an even n which is not a power of 2. Then they may subtract some odd divisor d, to get an odd number $n - d$ which is losing for their opponent.

In particular, as for (a), Alice wins for $n = 6$ and $n = 10$ but loses when $n = 8$.

Problem G6

A perfect power is an integer of the form b^n, where $b, n \geq 2$ are integers. Consider matrices 2×2 whose entries are perfect powers; we call such matrices *good.*

(a) Find an example of a good matrix with determinant 2019.

(b) Do there exist any such matrices with determinant 1? If so, comment on how many there could be. (Possible hint: use the theory of Pell equations.)

Solution

For (a), since $2019 = 3 \cdot 673 = 338^2 - 335^2$, we find that $\begin{bmatrix} 2^2 & 67^2 \\ 5^2 & 169^2 \end{bmatrix}$ is one such example.

For (b), the matrix $\begin{bmatrix} 4 & 27 \\ 25 & 169 \end{bmatrix}$ is one such example, found by using $25 \cdot 27 = 26^2 - 1$. Another example is $\begin{bmatrix} 33^2 & 8 \\ 35^2 & 9 \end{bmatrix}$. More generally, if $m \geq 1$ is an integer and

$$\left(3 + 2\sqrt{2}\right)^{2m+1} = 3x_m + 2y_m\sqrt{2}$$

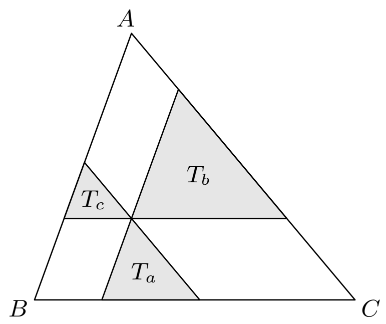
for integers x_m and y_m, then $9x_m^2 - 8y_m^2 = 1$ by multiplying by the conjugate (or by Pell equations). Thus

$$\det \begin{bmatrix} x_m^2 & 8 \\ y_m^2 & 9 \end{bmatrix} = 1$$

and so there are infinitely many examples.

Problem G7

We consider a fixed triangle ABC with side lengths $a = BC$, $b = CA$, $c = AB$, and a variable point X in the interior. The lines through X parallel to $\overline{AB}$ and $\overline{AC}$, together with line $\overline{BC}$, determine a triangle T_a. The triangles T_b and T_c are defined in a similarly way, as shown in the figure.



Let S and p denote the average area and perimeter, respectively, of the three triangles T_a, T_b, T_c.

(a) Determine all possible values of S as X varies, in terms of a, b, c.

(b) Determine all possible values of p as X varies, in terms of a, b, c.

Solution

For (a), we let X have barycentric coordinates (x, y, z) with respect to $\triangle ABC$, subject to $x + y + z = 1$. Letting brackets denote area, note that

$$[T_a] + [T_b] + [T_c] + [ABC] = \left((1-x)^2 + (1-y)^2 + (1-z)^2\right)[ABC]$$

since $(1-x)^2[ABC]$ corresponds to the area of the triangle formed by lines AB, AC, and the line through X parallel to $\overline{BC}$. Thus, we have

$$S = \frac{(1-x)^2 + (1-y)^2 + (1-z)^2 - 1}{3} \cdot [ABC].$$

We claim that S achieves its minimum when $x = y = 1/3$. To see this, write $(1-x)^2 + (1-y)^2 + (x+y)^2 = x^2 - x + (x-1)y + y^2$; for any given x this is minimal when $y = \frac{1-x}{2}$, and so substituting and minimizing x we find $x = y = 1/3$. Alternatively, one can simply apply Jensen's inequality on the function $t \mapsto (1-t)^2$,

Either way, we achieves a minimum value of

$$\frac{3 \cdot (2/3)^2 - 1}{3} \cdot [ABC] = \frac{1}{9}[ABC]$$

when X is the centroid of triangle ABC. Also, as $x \to 1^-$ and $y, z \to 0^+$ the value of S approaches $\frac{1}{3}[ABC]$ (and this is clearly best possible, since $[T_a] + [T_b] + [T_c] < [ABC]$ at all times). Thus for continuity reasons the answer to (a) is

$$S \in \left[\frac{[ABC]}{9}, \frac{[ABC]}{3}\right).$$

Here $[ABC] = \sqrt{\frac{1}{16}(a+b+c)(-a+b+c)(a-b+c)(a+b-c)}$ by Heron's formula.

For (b), the value of p is always equal to one-third of the perimeter of $\triangle ABC$, i.e. $p = \frac{1}{3}(a+b+c)$. Note that the sides of T_a, T_b, T_c which are parallel to $\overline{BC}$ have length summing to the length of BC. Consequently, the total perimeter coincides with that of $\triangle ABC$.

Solution to Advanced Math Problems

Problem M1

Let $\alpha = \sqrt{2} + \sqrt{3}$ and let $V = \mathbb{Q}(\alpha)$ be the field generated by α over $\mathbb{Q}$, regarded as a $\mathbb{Q}$-vector space. Let $T\colon V \to V$ be given by multiplication by α.

(a) Find $\dim V$.

(b) Let $W = \sqrt{2}\mathbb{Q} \oplus \sqrt{3}\mathbb{Q}$. Show that $V = W \oplus T(W)$. Give a basis of $T(W)$.

(c) Compute the determinant of T.

Solution

For (a), we have $\dim V = 4$. Here are two ways to see this:

- Since α has minimal polynomial $P(X) = (X^2 - 5)^2 - 24$ (irreducible over $\mathbb{Z}$), we have a basis $\{1, \alpha, \alpha^2, \alpha^3\}$.
- Alternatively, we note that $V \ni \frac{1}{2}(\alpha^2 - 5) = \sqrt{6}$. Then $\sqrt{6}\alpha = 2\sqrt{3} + 3\sqrt{2}$, and accordingly $(\sqrt{6} - 2)\alpha = \sqrt{2}$ and $(3 - \sqrt{6})\alpha = \sqrt{3}$ are also in V. As the numbers $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ are linearly independent over $\mathbb{Q}$ (and clearly span V), they form another basis of V.

Using the latter basis, it's easy to see that $V = W \oplus T(W)$, since $W = \sqrt{2}\mathbb{Q} \oplus \sqrt{3}\mathbb{Q}$, then

$$T(W) = (\sqrt{2}\alpha)\mathbb{Q} \oplus (\sqrt{3}\alpha)\mathbb{Q} = \left(2 + \sqrt{6}\right)\mathbb{Q} \oplus \left(3 + \sqrt{6}\right)\mathbb{Q} = \mathbb{Q} \oplus \sqrt{6}\mathbb{Q}$$

and in particular a basis of $T(W)$ is simply $\{1, \sqrt{6}\}$.

Those familiar with algebraic number theory may recognize $\det T = 1$ immediately as the product of the roots of $P(X)$. One can also do this computation in the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ in which T takes the matrix form

$$T = \begin{bmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

and $\det T = 1$.

Problem M2

Let n be a positive integer. We denote by I_n the $n \times n$ identity matrix. Let G be a group of $n \times n$ matrices with real entries and determinant 1 (under matrix multiplication).

Suppose that any sequence of matrices in G which converges to I_n is eventually constant. Show that for any $A > 0$, the subset of G with entries in $[-A, A]$ is finite.

Solution

The condition states that I_n is an isolated point of G.

Assume for contradiction that for some $A > 0$, there are infinitely many matrices in G with all entries bounded by A. Then, by Bolzano-Weierstrass theorem (applied on the n^2 entries), there should exist an infinite sequence $\gamma_1, \gamma_2, \ldots$ of distinct matrices in G which converges to some matrix ρ. Since $\det(\gamma_i) = 1$ for each i, it follows $\det \rho = 1$ as well.

Then the sequence $\gamma_n \gamma_{n+1}^{-1}$ (in G) converges to the identity matrix I_n. However, since I_n is an isolated point, it follows that $\gamma_n = \gamma_{n+1}$ for all large enough n, contradicting the assumption the γ_i were distinct.

Remark M2.1. The converse is also obviously true, and both conditions are equivalent to G being a discrete subgroup of $\mathrm{SL}_n(\mathbb{R})$. For $n = 2$, such a group is called a *Fuchsian group*, which arises in the study of modular forms.

Problem M3

(a) If $d \geq 0$ is an integer, evaluate

$$\lim_{n\to\infty} \int_{[0,1]^n} \left[\frac{x_1^2 + \cdots + x_n^2}{n}\right]^d \, \mathrm{d}x_1 \ldots \mathrm{d}x_n.$$

(b) Evaluate

$$\lim_{n\to\infty} \int_{[0,1]^n} \cos\left[\frac{x_1^2 + \cdots + x_n^2}{n} \cdot \pi\right] \, \mathrm{d}x_1 \ldots \mathrm{d}x_n.$$

Solution

We first show the answer to (a) is $(1/3)^d$, and state this explicitly as the following lemma.

Lemma M3.1. *For any integer $d \geq 0$,*

$$\lim_{n\to\infty} \int_{[0,1]^n} \left[\frac{x_1^2 + \cdots + x_n^2}{n}\right]^d \, \mathrm{d}x_1 \ldots \mathrm{d}x_n = \left(\frac{1}{3}\right)^d.$$

Proof. To see this, fix d and consider expanding the multinomial coefficient. There will be some terms of the form

$$d! \int_{[0,1]^n} x_{i_1}^2 x_{i_2}^2 \ldots x_{i_d}^2 = \left(\frac{1}{3}\right)^d$$

where $i_1 < i_2 < \cdots < i_d$. The number of such terms is $\binom{n}{d} = \frac{n^d}{d!} + O(n^{d-1})$. There are other terms where x_i's are repeated, but the contribution of each such term is clearly bounded by 1 and there are $O(n^{d-1})$ such terms as well. This proves the claim. $\square$

The answer to (b) is 1/2. We contend that:

Lemma M3.2. *For any continuous function $f\colon [0,1] \to \mathbb{R}$,*

$$\lim_{n} \int_{[0,1]^n} f\left(\frac{x_1^2 + \cdots + x_n^2}{n}\right) = f(1/3).$$

Proof. The Stone-Weierstrass theorem implies we can approximate the function f by a series $f(x) = \sum_d a_d x^d$, and the above lemma implies that

$$\int_{[0,1]} \sum_d a_d \left(\frac{x_1^2 + \cdots + x_n^2}{n}\right)^d = \sum_d a_d (1/3)^d = f(1/3). \qquad \square$$

Picking $f(t) = \cos(t\pi)$, we get the answer $f(1/3) = \cos(\pi/3) = \frac{1}{2}$.

Remark M3.3. This is related to the law of large numbers: consider the random variable X distributed as $t^2\ dt$ for $t \in [0,1]$. Then $\int_{[0,1]^n} \frac{x_1^2+\cdots+x_n^2}{n}$ corresponds to the mean when X is sampled n times, and thus "converges rapidly" to 1/3 as $n \to \infty$.

Problem M4

Let n be a fixed positive integer. We choose positive integers $t_1, \ldots, t_n$ (not necessarily distinct) and for each integer r, we let a_r denote the number of subsets $I \subseteq \{1, \ldots, n\}$ for which $\sum_{i \in I} t_i = r$ (this includes $I = \varnothing$ when $r = 0$). Consider the sum

$$\sum_{r \in \mathbb{Z}} a_r^2.$$

(a) Find the minimum possible value of this sum over all choices of $(t_1, \ldots, t_n)$, as a function of n.

(b) Find the maximum possible value of this sum over all choices of $(t_1, \ldots, t_n)$, as a function of n. (Possible hint: Sperner's theorem.)

Solution

We claim that the best bounds are

$$2^n \le \sum_r a_r^2 \le \binom{2n}{n}.$$

The quantity $\sum_r a_r^2$ counts the number of pairs of subsets (I, J) such that $\sum_{i \in I} t_i = \sum_{j \in J} t_j$. We call such pairs *good*.

The lower bound is clear, since pairs with $I = J$ are always good Equality can be achieved by letting $t_k = 2^k$ for every k so that these are the only such good pairs.

The upper bound is achieved by letting $t_k = 1$ for all k, so we now prove that this is the largest possible. There is a correspondence between pairs (I, J) and

$$K(I, J) = I \cup (\overline{J} + n) \subseteq \{1, \ldots, 2n\}$$

where $\overline{J}$ is the complement of J in $\{1, \ldots, n\}$. Under this correspondence, (I, J) if and only if

$$\sum_{k \in K(I,J)} t_k = t_1 + \cdots + t_n.$$

where we define $t_{n+1} = t_1$, $t_{n+2} = t_2$, $\ldots$, $t_{2n} = t_n$.

Because the t_i were given to be positive, no $K(I, J)$ from good (I, J) can be a subset of another. By Sperner's theorem, there are at most $\binom{2n}{n}$ of them.

Remark M4.1. This question was suggested by Ankan Bhattacharya.

Problem M5

Exhibit a function $s\colon \mathbb{Z}_{>0} \to \mathbb{Z}$ with the following property: if a and b are positive integers such that $p = a^2 + b^2$ is an odd prime, then

$$s(a) \equiv a^{\frac{p-1}{2}} \pmod p.$$

The right-hand side is known as the *Jacobi symbol* $\left(\frac{a}{p}\right)$.

Solution

Note $\gcd(a,p) = 1$. We recognize $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ as the Legendre symbol, and in fact we claim that

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \equiv 1 \pmod 2 \\ +1 & a \equiv 0 \pmod 4 \\ -1 & a \equiv 2 \pmod 4. \end{cases}$$

Thus we may take $s\colon \mathbb{Z}_{>0} \to \{-1, 1\}$ as above.

To prove this identity, we henceforth assume $p \equiv 1 \pmod 4$. Our proof will use extensively the Jacobi symbol and quadratic reciprocity.

First, assume a is odd. Then

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = +1.$$

Next, assume $a = 2x$ for x odd. Then $p \equiv 5 \pmod 8$, so $\left(\frac{2}{p}\right) = -1$. Then

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{x}{p}\right) = -1 \cdot \left(\frac{p}{x}\right) = -1.$$

Finally, assume $a = 2^e y$ for $e \ge 2$, and y odd. Then $p \equiv 1 \pmod 8$, so $\left(\frac{2}{p}\right) = 1$. Then

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^e \left(\frac{y}{p}\right) = \left(\frac{p}{y}\right) = +1.$$

Remark M5.1. Assuming there are infinitely many primes of the form $a^2 + b^2$ for any fixed $a > 0$ (which seems almost certainly true, although it is open), then the function s we gave above is the only one.

Problem M6

Let G be a nontrivial finite group. We consider automorphisms of G which do not preserve any nontrivial subgroup of G. (An automorphism *preserves* a subgroup of G if the image of that subgroup is itself.)

(a) Determine for which abelian groups G such an automorphism exists.

(b) Find the number of such automorphisms for each such G.

(c) Show that no such automorphisms exist if G is solvable but not abelian.

(d) Generalizing (c), prove that no such automorphisms exist if G is not abelian.

Solution

We begin by addressing (a), (c), (d) simultaneously.

Lemma M6.1 (Miklós Schweitzer 1985)**.** *Let G be any finite group (not necessarily abelian). No such automorphisms exist at all unless (and only unless) G is an elementary abelian group, that is, $G = (\mathbb{Z}/p)^{\oplus n}$.*

Proof. Let f be such an automorphism. Note that if f has a nontrivial fixed point, then f fixes the cyclic group generated by that fixed point, consequently G must be a cyclic group, at which point it is easy to see that G should be have prime order.

Thus, we may assume henceforth that f has no nontrivial fixed points. In that case, the map

$$G \to G \quad \text{by} \quad x \mapsto x^{-1} f(x)$$

is a bijection, since if $x^{-1}f(x) = y^{-1}f(y)$ then $f(yx^{-1}) = yx^{-1}$.

Now let p be any prime dividing G and let K be a Sylow p-group for G. As $f(K)$ must be a Sylow p-group as well, it is conjugate to K and consequently we have

$$f(K) = xKx^{-1}$$

for some $x \in G$. Now, pick y such that $f(y)x = y$ (possible by the previous claim); then

$$f(yKy^{-1}) = (f(y)x)K(f(y)x)^{-1} = yKy^{-1}.$$

So yKy^{-1} is a preserved subgroup of G. Consequently, $yKy^{-1} = G$, so G is a p-group (i.e. a group whose order is a prime power).

We remark that the p-group G has to be abelian, since the center of a p-group is characteristic and nontrivial. Finally, since the elements of order p form a nontrivial characteristic subgroup of G as well, so we conclude that G is an elementary abelian group. $\square$

As for $G = (\mathbb{Z}/p)^{\oplus n}$, viewing it as a n-dimensional vector space over $\mathbb{Z}/p$, an automorphism of G is equivalent to a invertible linear transformation T of G which has no proper nontrivial T-invariant subspaces. We relate this to the characteristic polynomial in the following way.

Lemma M6.2. *Let $T\colon V \to V$ be a map of finite-dimensional vector spaces. Then T has no proper nontrivial T-invariant subspaces if and only if the characteristic polynomial χ_T is irreducible.*

Proof. If χ_T is irreducible, there can be no T-invariant subspace since otherwise the restriction of T to that subspace gives a factor of the characteristic polynomial.

We now proceed conversely. Assume there are no T-invariant subspaces. Then the minimal polynomial μ_T of T should coincide with χ_T, since if not there exists a vector v such that the cyclic subspace spanned by $\{v, T(v), T(T(v)), \dots\}$ has dimension $\dim \mu_T$, and hence is a nontrivial proper T-invariant subspace.

In that case, we can pick a basis of V so that it coincides with the companion matrix for χ_T. Then $V \cong \mathbb{F}_p[X]/(\chi_T(X))$ as $\mathbb{F}_p[T]$-modules, and so the invariant subspaces of V are in bijection with the nontrivial factors of χ_T. $\square$

For the count, we quote two results.

Lemma M6.3 (Gauss formula)**.** *There are $\frac{1}{n}\sum_{d|n}\mu(n/d)p^d$ monic irreducible polynomials of degree n over $\mathbb{F}_p$.*

Lemma M6.4 (Reiner, Gerstenhaber, 1960)**.** *For a given irreducible polynomial f, the number of $n \times n$ matrices over $\mathbb{F}_p$ with characteristic polynomial f is $\prod_{i=1}^{n-1}\left(p^n - p^i\right)$.*

For references on these two results, see:

- `https://arxiv.org/pdf/1001.0409.pdf`,
- `http://math.sun.ac.za/wp-content/uploads/2012/09/tovo.pdf`,

respectively.

Return to the situation $G = (\mathbb{Z}/p)^{\oplus n}$. When $n = 1$ the answer is just the number of automorphisms, which is $p - 1$ (the matrix $\begin{bmatrix}0\end{bmatrix}$ has no proper invariant subspace but is not invertible). For $n \geq 2$, any T with no invariant subspace is necessarily invertible as well, giving the final answer

$$\frac{1}{n}\left(\sum_{d|n}\mu(n/d)p^d\right)\left(\prod_{i=1}^{n-1}\left(p^n - p^i\right)\right).$$