Why are numbers beautiful? It’s like asking why is Beethoven’s Ninth Symphony beautiful. If you don’t see why, someone can’t tell you. I know numbers are beautiful. If they aren’t beautiful, nothing is.

Paul Erdős

1 Rules and Reminders

These rules supersede any rules appearing elsewhere about the Power Round:

1. On any problem, you may use without proof any result or remark from earlier in the test, even if it’s a problem your team has not solved. You may cite results from conjectures or subsequent problems only if your team solved them independently of the problem where you wish to cite them.

2. You may not cite parts of your proof of other problems: if you wish to use a lemma in multiple problems, please reproduce it in each one.

3. It is not necessary to do the problems in order, although it is a good idea to read all the problems, so that you know what is permissible to assume when doing each problem. However, please collate the solutions in order in your solution packet. Each problem should start on a new page, and solutions should be written on one side of the paper only. Each page should also have on it the team name and problem number.

4. Using computer programs, calculators, and Mathematica (or similar programs), is allowed. However, print and online references are not allowed.

5. No communication with humans outside your team about the content of these problems is allowed. If you have any questions regarding the test, please contact us at once at pumac@math.princeton.edu
2 Background

We write
1. \( \mathbb{N} \) for the set of positive integers.
2. \( \mathbb{Z} \) for the set of integers.
3. \( \mathbb{Q} \) for the set of rational numbers.
4. \( \mathbb{C} \) for the set of complex numbers.

2.1 A Little Number Theory Background

**Definition 1** (Congruence). Let \( a, b, n \) be integers with \( n \neq 0 \). We say that \( a \) and \( b \) are congruent modulo \( n \) if \( n | a - b \), and denote this by \( a \equiv b \) (mod \( n \)). If \( n \nmid a - b \), we say that the integers \( a, b \) are not congruent modulo \( n \) and write \( a \not\equiv b \) (mod \( n \)).

For instance, \( 7 \equiv 1 \) (mod 3), and \( 23 \not\equiv 2 \) (mod 5).

**Remark.** It is known (and very easily verified) that the congruence relation defined above is an equivalence relation that satisfies the following properties:
1. \( a \equiv a \) (mod \( n \)) (reflexivity);
2. If \( a \equiv b \) (mod \( n \)) and \( b \equiv c \) (mod \( n \)), then \( a \equiv c \) (mod \( n \)) (transitivity);
3. If \( a \equiv b \) (mod \( n \)), then \( b \equiv a \) (mod \( n \)) (symmetry);
4. If \( a \equiv b \) (mod \( n \)) and \( c \equiv d \) (mod \( n \)), then \( ka + lc \equiv kb + ld \) (mod \( n \)) for all integers \( k, l \in \mathbb{Z} \).
5. If \( a \equiv b \) (mod \( n \)) and \( c \equiv d \) (mod \( n \)), then \( ac \equiv bd \) (mod \( n \)).
6. If \( ka \equiv kb \) (mod \( n \)) and \( \gcd(k, n) = d \), then \( a \equiv b \) (mod \( \frac{n}{d} \)).

In general, a binary relation \( a \equiv b \) is called an equivalence relation if it satisfies reflexivity, symmetry and transitivity.

The following theorems may be helpful.

**Theorem 2** (Fermat’s Little Theorem). Let \( a \) be a positive integer and let \( p \) be a prime such that \( (a, p) = 1 \). Then

\[
a^{p-1} \equiv 1 \quad \text{(mod } p)\text{.}
\]

**Proof.** Fix an integer \( a \) such that \( (a, p) = 1 \). Note that the integers \( a, 2a, \cdots, (p-1)a \) are all distinct modulo \( p \), so up to a permutation, the sets \( \{a, 2a, \cdots, (p-1)a\} \) and \( \{1, 2, \cdots, p-1\} \) are congruent. This means that their products are congruent modulo \( p \), that is,

\[
(p-1)!a^{p-1} \equiv (p-1)! \quad \text{(mod } p)\text{.}
\]

Cancelling \((p-1)!\) from both sides (this is possible because \((p-1)!\) is coprime to \( p \)), we have the desired equality \( a^{p-1} \equiv 1 \) (mod \( p \)) immediately.
An important question throughout the process of this Power Round would be whether the congruence \( x^2 \equiv a \pmod{p} \) has a solution \( x \in \mathbb{Z} \) given an integer \( a \) and a prime \( p \). The following concept will be extremely helpful.

**Definition 3** (Quadratic residue). Let \( a \) and \( m \) be integers such that \( m > 0 \). We say that \( a \) is a quadratic residue mod \( m \) if the congruence \( x^2 \equiv a \pmod{m} \) has a solution. Otherwise we say that \( a \) is a quadratic nonresidue.

**Remark.** 0, 1, 4 are quadratic residues modulo 5. 0, 1, 2, 4 are quadratic residues modulo 7. 0, 1, 4 are quadratic residues modulo 8.

The following notation will be useful.

**Definition 4.** Let \( p \) be an odd prime and let \( a \) be an integer not divisible by \( p \). The Legendre symbol of \( a \) with respect to \( p \) is defined by

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ a quadratic residue modulo } p \\
-1 & \text{otherwise}
\end{cases}
\]

**Remark.** The Legendre symbol satisfies the following properties.

1. There are \( \frac{p-1}{2} \) quadratic residues in the set \{1, 2, \cdots, p-1\}. (Proof: \( \{1^2, 2^2, \cdots, (\frac{p-1}{2})^2\} \) are distinct mod \( p \) and \( x^2 \equiv (p-x)^2 \pmod{p} \))

2. (Euler’s criterion) If \( p \) is an odd prime and \( a \) an integer not divisible by \( p \), then

\[
\left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p}.
\]

(Try proving using Fermat’s little theorem!)

3. If \( a \equiv b \pmod{p} \), then \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \)

4. (multiplicity) \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \)

**Theorem 5** (Quadratic Reciprocity). Given two odd primes \( p \neq q \), we have

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}.
\]

Stated differently, \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \) unless \( p \equiv q \equiv 3 \pmod{4} \).

**2.2 Background for This Year’s Power Round**

This year’s Power Round concerns the following interesting mathematical object.
Definition 6 (Conic Polynomial). A Conic Polynomial involving \( n \) variables \( X_1, X_2, \cdots, X_n \) is the homogeneous polynomial

\[
f = f(X_1, X_2, \cdots, X_n) = \sum_{1 \leq i,j \leq n} a_{i,j} X_i X_j
\]

where \( a_{i,j} \) are real numbers and the sum ranges over all pairs \((i, j)\) with \(1 \leq i \leq n\) and \(1 \leq j \leq n\).

We may write this conic polynomial in the following matrix notation:

\[
f = X^T A X = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}
\]

We say that a conic polynomial \( f \) is integral if for all integers \( X_1, X_2, \cdots, X_n \), \( f(X_1, X_2, \cdots, X_n) \) is also an integer.

We can easily see that the forms \( x^2 + 3xy + 5y^2 \), \( x^2 - y^2 \) are two-variable integral conic polynomials, and \( x^2 + y^2 + z^2 \), \( xy + xz \) are three-variable integral conic polynomials.

Definition 7. Multiple matrices may be associated with the same conic polynomial. For example, the conic polynomial \( x^2 + 4xy + y^2 \) can be associated with the two matrices

\[
A_1 = \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}
\]

and

\[
A_2 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.
\]

However, there is a unique way to associate a conic polynomial with a symmetric matrix \( A = (a_{i,j}) \) with \( a_{i,j} = a_{j,i} \). For example, \( x^2 + 4xy + y^2 \) is associated to the following matrix

\[
A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.
\]

We call this matrix the symmetric matrix associated to a conic polynomial \( f \). If the symmetric matrix associated to a conic polynomial \( f \) has integer entries, we say that \( f \) has integer matrix.

Definition 8. We say that a conic polynomial \( f(X_1, X_2, \cdots, X_n) \) is integral if \( f(X_1, X_2, \cdots, X_n) \) is an integer for all integers \( X_1, X_2, \cdots, X_n \). Note that this is not equivalent to the fact that \( f \) has integer matrix.

Definition 9. We say that a conic polynomial \( f(X_1, X_2, \cdots, X_n) \) represents an integer \( d \in \mathbb{Z} \) if \( f(X_1, X_2, \cdots, X_n) = d \) has a solution with \( X_i \in \mathbb{Z} \) for all \( i \).
Definition 10. We say that a conic polynomial \( f \) is positive-definite if \( f \geq 0 \) for all integer inputs and \( f = 0 \) iff all arguments are zero.

Definition 11. We say that a positive-definite conic polynomial \( f \) is universal if \( f \) represents all nonnegative integers.

Let’s begin by gaining some intuition on these conic polynomial, and get used to the definitions.

Problem 1. (8 points)

1. (3) Show that a conic polynomial
\[
f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j
\]
is integral if and only if \( a_{i,i} \in \mathbb{Z} \) and \( a_{i,j} + a_{j,i} \in \mathbb{Z} \).

2. (1) Find an integral conic polynomial that does not have integer matrix.

3. (1) Find a conic polynomial with two or less variables that can represent all integers.

4. (3) What integers can the following conic polynomials represent? A good answer should (1) be exhaustive (should not leave out representable integers), (2) be correct (should not say an integer is representable when it’s not), (3) prove 1 and 2 (the proof can be concise).
   
   (a) \( f(x, y) = x^2 - y^2 \)
   
   (b) \( f(x, y) = x^2 - 4xy + 4y^2 \)
   
   (c) \( f(x, y, z) = x^2 - y^2 + z^2 \)

3 Binary Conic Polynomial

Definition 12. A binary conic polynomial is a conic polynomial with two variables. It may be written in the form \( ax^2 + bxy + cy^2 \).

In this section, we will look at examples of how binary conic polynomials can represent positive integers. We focus our attention on positive-definite binary conic polynomials.

We first look at a canonical example: \( x^2 + y^2 \).

Problem 2. (15 points)

1. (2) Assume positive integers \( m, n \) are both representable by the conic polynomial \( f(x, y) = x^2 + y^2 \). Show that so is \( mn \).

2. (2) If \( p \) is a prime of the form \( 4k + 3 \), show that \( p|x^2 + y^2 \) implies \( p|x \) and \( p|y \).
3. (2) If \( p \) is a prime of the form \( 4k + 1 \), show that \( t^2 \equiv -1 \pmod{p} \) has a solution \( t \in \mathbb{Z} \).

4. (5) If \( p \) is a prime of the form \( 4k + 1 \), show that \( p \) is representable by the conic polynomial \( f(x, y) = x^2 + y^2 \).

(Hint: Prove and use the following lemma on the solution \( t \) of the previous problem.

Lemma. Given an odd prime \( p \) and an integer \( t \), the following congruence

\[
tx + y \equiv 0 \pmod{p}
\]

has a solution \((x, y)\) with \(0 \leq |x| < \sqrt{p}, 0 \leq |y| < \sqrt{p}, (x, y) \neq (0, 0)\).)

5. (4) Classify all positive integers that can be represented by the form \( f(x, y) = x^2 + y^2 \).

We look at more examples that can be proved with similar techniques.

**Problem 3.** (20 points)

1. (10) Classify all positive integers that can be represented by the form \( f(x, y) = x^2 + 2y^2 \).

2. (10) Classify all positive integers that can be represented by the form \( f(x, y) = x^2 + 3y^2 \).

Note that the form \( x^2 + y^2 \) will represent the same set of integers as the form \( x^2 + (x+y)^2 = 2x^2 + 2xy + y^2 \). However, we also note that the form \( x^2 + y^2 \) does not represent the same set of integers as the form \( x^2 + (x+3y)^2 = 2x^2 + 6xy + 9y^2 \). (Why?)

With this intuition, we define the notion of equivalence among binary conic polynomial as follows.

**Definition 13.** Given a binary conic polynomial \( f(x, y) \), we say that \( F(x, y) = f(ax + by, cx + dy) \) is equivalent to \( f \) if \( |ad - bc| = 1 \).

**Problem 4.** (5 points)

1. (3) Show that this defines an equivalence relation over binary conic polynomials: that is, the equivalence relation is reflexive, symmetric, and transitive. (See the definition of congruence above for what these words mean.)

2. (2) Show that two binary conic polynomials are equivalent only if they represent the same set of integers.

We define the discriminant of a binary conic polynomial as follows:

**Definition 14.** Given a binary conic polynomial \( f(x, y) = ax^2 + bxy + cy^2 \), we define its discriminant \( D(f) = b^2 - 4ac \).

**Problem 5.** (10 points)
1. (1) Assume that \( D(f) < 0 \) and \( a > 0 \). Prove that \( f \) is positive-definite. Does the converse hold?

2. (3) Assume that \( f(x, y) = ax^2 + bxy + cy^2 \) represents a prime \( p \). Show that \( D(f) \) is a quadratic residue modulo \( p \).

3. (6) Show that equivalent binary conic polynomials have the same discriminant. Does the converse hold?

**Problem 6.** (31 points) (Miscellaneous problems)

These problems are intended to give you better intuition about representations of integers with conic polynomials. Have fun, do not be intimidated - even Fermat and Euler had a hard time with this theory!

1. (2) Given an odd prime number \( p \), show that

\[
\left( \frac{-5}{p} \right) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}.
\]

Does it imply that every such prime may be written in the form \( x^2 + 5y^2 \) for integers \( x, y \)? (This contrasts with some previous problems)

2. (3) Prove that if \( \left( \frac{-5}{p} \right) = 1 \) for an odd prime \( p \), then either \( p \) or \( 2p \) can be represented by \( x^2 + 5y^2 \).

3. (5) For an odd prime \( p \) such that \( \left( \frac{-23}{p} \right) = 1 \), show that either \( p \) or \( 3p \) can be represented by the form \( x^2 + 23y^2 \). Does the converse hold?

4. (3) In a previous problem, we showed that \( x^2 + y^2 = p \) has a solution for primes \( p \) congruent to 1 modulo 4. Is this representation unique? That is, assume we have \( a^2 + b^2 = c^2 + d^2 = p \). Must it be the case that \( \{a, b\} = \{c, d\} \)?

5. (5) Assume that a prime \( p \) can be written in the form \( 3x^2 + 7y^2 \). Show that this representation is unique for \( x, y \) non-negative.

6. (5) For pairwise relatively prime integers \( a, b, c \), consider the conic polynomial \( f(x, y) = ax^2 + bxy + cy^2 \). Given any positive integer \( M \), prove that you can find non-negative integers \( x_0, y_0 \) such that \( f(x_0, y_0) \) is relatively prime to \( M \).

7. (5) Given a positive integer \( n \) and coprime integers \( a, b \), write \( N = a^2 + nb^2 \). Assume that there exists a prime divisor \( q \) of \( N \) such that \( q = x^2 + ny^2 \) for \( x, y \in \mathbb{Z} \). Show that \( \frac{N}{q} = c^2 + nd^2 \) for \( (c, d \in \mathbb{Z}) \).

8. (3) Denote the subsets \( A, B \) of positive integers as follows:

\[
A = \{n \mid n < 2^{2000}, n = 2x^2 - 3y^2 \text{ for some } x, y \in \mathbb{Z} \}
\]
\[
B = \{n \mid n < 2^{2000}, n = 10xy - x^2 - y^2 \text{ for some } x, y \in \mathbb{Z} \}
\]

Determine which of \( A \) or \( B \) is larger.

7
4 A Conic Polynomial Expressing All Integers

In this section we attempt at finding a positive-definite square: namely, \( x^2 + y^2 + z^2 + w^2 \).

**Problem 7.** (20 points) In this section, denote by \( f(x, y, z, w) \) the positive-definite conic polynomial \( x^2 + y^2 + z^2 + w^2 \).

1. (3) Show that if integers \( m, n \) can be represented by \( f \), then so can \( mn \).

2. (5) Given an odd prime number \( p \), show that there exists an positive integer \( t < p \) such that \( tp \) can be represented by \( f \).

3. (2) If \( t_0 \) is the smallest positive integer \( t \) such that \( t_0 p \) can be represented by \( f \), show that \( t_0 \) is odd.

4. (5) Given \( t_0 \) as above, if \( t_0 > 1 \), show that \( st_0 \) can be represented by \( f \) for some positive integer \( s < t_0 \).

5. (3) Show that \( t_0 = 1 \). (So the statement above was actually vacuously true. But using the above statement will probably help!)

6. (2) Show that every positive integer can be represented by \( f \).

In fact, it can be shown that more than 40 forms of the form \( ax^2 + by^2 + cz^2 + dw^2 \) can represent all nonnegative integers - we investigate this further in subsequent sections.

5 Ternary Conic Polynomial

Now that we have seen an example of a universal positive-definite conic polynomial, we dig deeper into analyzing conic polynomials. Much has been discussed about polynomials of two variables, and you may have noticed that two-variable conic polynomials represent a small subset of the positive integers. In the three-variable case, however, it is different – it represents a substantial portion of the positive integers. Let’s see how it goes.

**Definition 15.** A ternary conic polynomial is a conic polynomial \( f(x, y, z) \) with three variables.

Much of the facts about ternary conic polynomials is not elementary - it requires extensive use of theories beyond the number theory most of you know. Everything here, with a bit of hints tho, are approachable with elementary number theory. Good luck!

For this section and this section ONLY, you may use the following theorem to your advantage:

**Theorem 16** (Dirichlet’s Theorem on Arithmetic Progressions). If \( a, b \) are positive integers such that \( (a, b) = 1 \), there are infinitely many primes of the form \( an + b \) where \( n \in \mathbb{Z} \).
We first look at the "basic" ternary form $x^2 + y^2 + z^2$.

**Problem 8.** (55 points)

1. (5) Let $n = 4^m(8k + 7)$ for nonnegative integers $m, k$. Prove that $n$ cannot be represented by $x^2 + y^2 + z^2$.

2. (15) Given an integer $n$, assume that the equation $n = x^2 + y^2 + z^2$ has rational solutions $(x, y, z)$. Prove that the equation has a solution with $x, y, z$ integers.

3. (10) Given a squarefree integer $m \equiv 1 \pmod{4}$, show that you can choose a prime $q$ of the form $4k + 1$ such that $-q$ is a quadratic residue mod $m$ and $m$ is a quadratic residue mod $q$.

4. (5) Do the same for $m \equiv 2 \pmod{4}$.

5. (10) Given a squarefree integer $m \equiv 3 \pmod{8}$, show that you can find a prime $q$ of the form $8k + 5$ such that $-2q$ is a quadratic residue mod $m$ and $m$ is a quadratic residue mod $q$.

6. (10) Using the three previous problems and Legendre’s theorem, show that a positive integer $m$ not of the form $4^l(8k + 7)$ is the sum of three rational squares. What can we say about the numbers that can be represented by the conic polynomial $f(x, y, z) = x^2 + y^2 + z^2$?

**Remark.** Legendre’s theorem is the following:

*Theorem 17 (Legendre’s theorem).* Given integers $a$ and $b$, the equation $z^2 = ax^2 + by^2$ has a nontrivial solution $(x, y, z)$ if and only if $a, b$ are not both negative, and $b$ is a quadratic residue mod $|a|$ and $a$ is a quadratic residue mod $|b|$.

It should be noted that this section solves the question posed at the previous section too! In fact, it proves more.

**Problem 9.** (5 points)

1. (5) Show that the conic polynomials $f(x, y, z, w) = x^2 + y^2 + z^2 + dw^2$ for $1 \leq d \leq 7$ are universal.

6 Universal Conic Polynomials

In this section we attempt to classify some universal conic polynomials. These will turn out to be a large portion of all universal conic polynomials!

**Problem 10.** (20 points)

1. (5) Assume that a conic polynomial $ax^2 + by^2 + cz^2 + dw^2$ is universal, and let $1 \leq a \leq b \leq c \leq d$. Show the following:
(a) \( a = 1 \)
(b) \( b \leq 2 \)
(c) When \( b = 1 \), \( c \leq 3 \), and when \( b = 2 \), \( c \leq 5 \).

2. (15) Given the following information:

(a) \( x^2 + y^2 + 2z^2 \) represents all integers not of the form \( 4^m(16n + 14) \)
(b) \( x^2 + y^2 + 3z^2 \) represents all integers not of the form \( 9^m(9n + 6) \)
(c) \( x^2 + 2y^2 + 2z^2 \) represents all integers not of the form \( 4^m(8n + 7) \)
(d) \( x^2 + 2y^2 + 3z^2 \) represents all integers not of the form \( 4^m(16n + 10) \)
(e) \( x^2 + 2y^2 + 4z^2 \) represents all integers not of the form \( 4^m(16n + 14) \)
(f) \( x^2 + 2y^2 + 5z^2 \) represents all integers not of the form \( 25^m(25n + 10) \)

or \( 25^m(25n + 15) \)

classify all universal conic polynomials of the form \( ax^2 + by^2 + cz^2 + dw^2 \).

7 Bonus Problems

This section asks problems that diverge from previous problems and look at more general polynomials. Hence they are, in some sense, irrelevant to the theory - hence the name. These are interesting problems that deserve attention tho!

1. (10) Show that every positive integer is the sum of two squares and a cube (of integers, not necessarily positive!).

2. (10) Show that every positive integer is the sum of three triangular numbers. Triangular numbers are \( T_n = 1 + 2 + \ldots + n \).