UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.

MATH5645: TOPICS IN NUMBER THEORY.

§0 INTRODUCTION:

Number Theory is essentially concerned with the properties of the natural numbers and the integers,

$$\mathbb{N} = \{0, 1, 2, 3, ...\}, \qquad \mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

The ancient Greeks studied some basic properties of numbers and Euclid describes some of these results in Book 10 of the *Elements.* Diophantus (c. 250 AD ??) studied certain equations (called *Diophantine Equations* in his honour) which may or may not have integer/rational solutions. Diophantus' work inspired Fermat (1601-1665), regarded as the 'founder' of modern number theory, to develop number theory as a systematic branch of learning. Major strides forward were taken by Euler and Gauss.
Nowadays, number theory is divided into a range of categories including:

- Algebraic Number Theory
- Analytic Number Theory
- Probabilistic Number Theory
- Geometric Number Theory

etc.

This course will deal with the rudiments of Classical and Analytic Number Theory.

§1 SOME CLASSICAL NUMBER THEORY:

Summary of basic facts

Notation:
For n a positive integer, we will use the notation $\mathbb{Z}_n$ to denote the ring of integers modulo n. In the case when n is a prime p, $\mathbb{Z}_p$ forms a field, and so each non-zero element has a multiplicative inverse. The invertible elements in the ring $\mathbb{Z}_n$ are those elements which are co-prime to n. These numbers are called the **units** in the ring, and the set of such elements is denoted by $\mathbb{U}_n$. Thus, $\mathbb{U}_{12} = \{1, 5, 7, 11\}$.

We will write (a, b) for $\gcd(a, b)$ and recall that if $d = (a, b)$ then $d = ax + by$ for some integers x, y.

Basic Theorems:

Linear Equations:

For n a positive integer and a, b integers, the linear congruence equation $ax \equiv b \mod n$ has solutions if and only if $d = (a, n)$ is a factor of b, in which case there are d mutually incongruent solutions modulo n.

The Chinese Remainder Theorem deals with simultaneous linear congruence equations. Thus, if $n_1, n_2, ..., n_k$ are pairwise coprime positive integers, then the system:

$$x \equiv a_1 \mod n_1$$

$$x \equiv a_2 \mod n_2$$

.....

$$x \equiv a_k \mod n_k$$

has a unique solution modulo $N = n_1 n_2 ... n_k$.

This result is very useful, since when dealing with a congruence equation of the form $f(x) \equiv 0 \mod n$, we can uniquely factor n into a product of prime powers and consider the congruence with respect to each prime power and finally recombine to obtain solutions if they exist.

Fermat's Little Theorem states that if p is prime and $p \not| a$ then

$$a^{p-1} \equiv 1 \mod p.$$

To generalise this we need Euler's phi function, $\phi(n)$, which equals the size of the set $\{x \in \mathbb{Z}^+ : 0 < x < n, (x, n) = 1\}$. Thus $\phi(12) = 4$.

For p prime, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Also, if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. These two facts allow us to find $\phi(n)$ for any positive integer n. For example:

$\phi(7878) =$

Euler's Theorem states that if $(a, m) = 1$, where $m \in \mathbb{Z}^+$, then

$$a^{\phi(m)} \equiv 1 \mod m.$$

The group $\mathbb{U}_n$ is cyclic if and only if $n = 1, 2, 4, p^\alpha, 2p^\alpha$, where p is an odd prime. In this case, there are $\phi(\phi(n))$ generators, often referred to as **primitive roots**. In the case when $n = p$, there are $\phi(p-1)$ primitive roots.

A number a has **order** k mod n means that k is the smallest positive integer such that $a^k \equiv 1 \mod n$. Thus a is a primitive root mod n if and only if a has order $\phi(n)$.

Wilson's Theorem.
p is prime iff $(p-1)! \equiv -1 \mod p$.

Corollary. Suppose p is a prime congruent to 1 mod 4. Then $x^2 \equiv -1$ has a solution.

Proof.

(Note that the converse is also true, i.e. with p an odd prime, $x^2 \equiv -1 \mod p$ has a solution only if $p \equiv 1 \mod 4$.)

The following two results are worth noting:

Theorem 1.1 Let n be an integer for which $\mathbb{U}_n$ admits primitive roots and suppose $(a, n) = 1$. Then the congruence $x^k \equiv a \mod n$ has a solution iff

$$a^{\frac{\phi(n)}{d}} \equiv 1 \mod n$$

where $d = \gcd(k, \phi(n))$. Furthermore, if it has solutions, then it has exactly d solutions in $\mathbb{U}_n$.

A special case, originally due to Euler, states:

Corollary: Suppose p is a prime and $(a, p) = 1$. Then the congruence $x^k \equiv a \mod p$ has solution iff $a^{(p-1)/d} \equiv 1 \mod p$, where $d = \gcd(k, p-1)$.

Quadratic Residues.

If $x^2 \equiv a \mod p$ has solution, that is, if a is a square in $\mathbb{Z}_p$, and $a \not\equiv 0$, then we say that a is a **quadratic residue** modulo p, q.r. for short, otherwise it is referred to as a **quadratic non-residue**, (q.n.r.).

For example, in $\mathbb{U}_{11}, \{1, 4, 9, 5, 3\}$ are the quadratic residues and $\{2, 6, 7, 8, 10\}$ are the non-residues.

Theorem 1.2:
For p a prime, exactly half of the numbers in $\mathbb{U}_p$ are quadratic residues.

Proof:
This is almost obvious, but the following proof contains a useful idea.

Euler's Criterion.

We want a simple test to determine when a given number a is a (non-zero) square in $\mathbb{Z}_p$. For example, is 3127 a square in $\mathbb{Z}_{12713}$?

Theorem 1.3:

If p is an odd prime, and $p \not| a$ then $x^2 \equiv a \mod p$ is solvable iff

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

(Hence a is a non-residue if $a^{\frac{p-1}{2}} \equiv -1 \mod p$.)

Proof: This is a special case of Theorem 1.1.

Example: Is 3 a q.r. in $\mathbb{Z}_{23}$?

Euler's criterion is a useful theoretical tool (as you will see in the tutorial problems), but for large moduli it is not very practical.

Legendre's Symbol:

We define the Legendre symbol by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a q.r.} \mod p \\ -1 & \text{if } a \text{ is a q.n.r.} \mod p \end{cases}$$

where $(a, p) = 1$.

we can now state Euler's theorem as $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Trivially, for $(a, p) = 1$ we have $\left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$ and for $p \equiv 1 \mod 4$, $\left(\frac{-1}{p}\right) = 1$.

Theorem 1.2 immediately implies that

$$\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$$

for any odd prime p.

The Legendre symbol has a number of simple properties which assist in its calculation:

Theorem 1.4: If $(a, p) = (b, p) = 1$, p an odd prime, then

(i) $a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof: Simple exercise.

Examples: Find $\left(\frac{19}{5}\right), \left(\frac{47}{17}\right), \left(\frac{5}{17}\right)$.

Gauss' Lemma.

There are still computational difficulties, for example, how do we find $\left(\frac{127}{3499}\right)$?

The key to evaluating Legendre symbols is Gauss' famous reciprocity law. Gauss gave a number of proofs of this, but all of them, with one exception, relied on the following rather strange result, known as Gauss' Lemma. (There is a wonderful two line proof (!) but this requires the machinery of characters and Gauss sums, which we will not have time to cover.)

Theorem 1.5: Gauss' Lemma.
Suppose that p is an odd prime and $(a, p) = 1$. Consider the set $S = \{a, 2a, ..., \frac{1}{2}(p-1)a\}$ with elements reduced modulo p. Let k be the number of elements in the reduced set S that are greater than $\frac{p-1}{2}$, then $\left(\frac{a}{p}\right) = (-1)^k$.

Proof:

Example: Use Gauss' Lemma to find $\left(\frac{5}{13}\right)$.

Example: Use Gauss' Lemma to show that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

for any odd prime p.

Example. Suppose q is an odd integer such that $p = 12q + 1$ is prime.
(i) Evaluate $\left(\frac{2}{p}\right)$

(ii) Use Euler's Criterion to show that $2^{6q} \equiv -1 \bmod p$.

(iii) Find a prime factor of $2^{78} + 1$.

The Law of Quadratic Reciprocity.

Theorem 1.6:

Suppose p, q are **odd** primes, then

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p \equiv 1 \mod 4$ OR $q \equiv 1 \mod 4$

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv 3 \mod 4$ AND $q \equiv 3 \mod 4$.

Equivalently,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Example: Evaluate $\left(\frac{521}{997}\right)$.

There are many proofs of the reciprocity theorem.

The following proof is due to Eisenstein, and attracted Gauss' high approval.

Lemma:
Let a be an **odd** integer and p a prime not dividing a.
Let

$$M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + ... + \left[\frac{\frac{1}{2}(p-1)a}{p}\right],$$

then $\left(\frac{a}{p}\right) = (-1)^M$.

Proof: Applying the method in Gauss' Lemma, we divide the elements of the set $\{a, 2a, ..., \frac{1}{2}(p-1)a\}$ by p and write

$$a = p\left[\frac{a}{p}\right] + r_1$$

$$2a = p\left[\frac{2a}{p}\right] + r_2$$

$$.....$$

$$\frac{1}{2}(p-1)a = p\left[\frac{a(p-1)/2}{p}\right] + r_{\frac{1}{2}(p-1)}.$$

Now add both sides to get

$$\frac{1}{8}(p^2-1)a = pM + r_1 + r_2 + ... + r_{\frac{1}{2}(p-1)}.$$

Now the remainders are all different (since $p \not| a$) and (as in the proof of Gauss' Lemma) we let $a_1, ..., a_k$ be those remainders which are $> \frac{1}{2}(p-1)$ and $a_{k+1}, ..., a_{\frac{1}{2}(p-1)}$ be the rest. Hence we can write the above equation as:

$$\frac{1}{8}(p^2-1)a = pM + a_1 + a_2 + ... + a_k + a_{k+1} + ... + a_{\frac{1}{2}(p-1)}. \qquad (*).$$

Now $p - a_1, p - a_2, ..., p - a_k$ will be less than $\frac{1}{2}(p-1)$ and so the set of numbers

$$\{p - a_1, p - a_2, ..., p - a_k, a_{k+1}, ..., a_{\frac{1}{2}(p-1)}\}$$

will just be the numbers $\{1, 2, 3, ..., \frac{1}{2}(p-1)\}$ (in some order). So adding these numbers we have

$$\frac{1}{8}(p^2-1) = kp - (a_1 + a_2 + ... + a_k) + a_{k+1} + ... + a_{\frac{1}{2}(p-1)}.$$

Subtracting this from equation (*) we have:

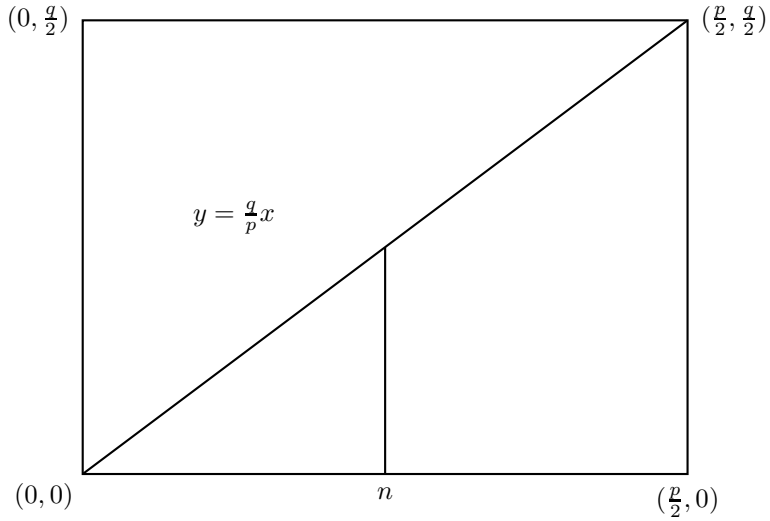
$$\frac{1}{8}(p^2-1)(a-1) = p(M-k) + 2a_1 + ... + 2a_k.$$

Since a is odd, $M - k$ is even so M and k are either both even or both odd and so $(-1)^k = (-1)^M$, and thus $\left(\frac{a}{p}\right) = (-1)^k = (-1)^M$.

Proof of Theorem 1.6:

Let $M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + ... + \left[\frac{\frac{1}{2}(p-1)q}{p}\right]$ and
$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + ... + \left[\frac{\frac{1}{2}(q-1)p}{q}\right]$, then by the Lemma, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N}$ and so we need to show that $M + N = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$.

Consider a rectangle R in the plane with vertices $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2}), (\frac{p}{2}, \frac{q}{2})$ as shown.



The rectangle R contains $\frac{1}{2}(p-1)\frac{1}{2}(q-1)$ lattice points excluding the boundary. The diagonal from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ has equation $y = \frac{q}{p}x$ and so for any positive integer $n < \frac{p}{2}$, $\left[\frac{nq}{p}\right]$ is the number of lattice points on the vertical line through the point $(n, 0)$ that lie on or below the diagonal. Now there are no lattice points on the diagonal since p, a prime, cannot cancel with any integer x less than $\frac{p}{2}$.

Thus M counts all the lattice points below that diagonal and similarly N counts all those above the diagonal and hence $N + M = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$ as claimed.

Example: Show that 5 is a q.r. for all primes of the form $p \equiv \pm 1 \mod 10$.

Example: Find all the primes for which 3 is a q.r. modulo p.

Sums of Integer Squares:

The numbers 8 and 90 can be expressed as the sum of two squares,

$$8 = 2^2 + 2^2 \qquad 90 = 3^2 + 9^2,$$

while we need three squares to represent 35,

$$35 = 5^2 + 3^2 + 1^2$$

and even three squares is not enough for 28 which is

$$28 = 5^2 + 1^2 + 1^2 + 1^2 = 3^2 + 3^2 + 3^2 + 1^2.$$

In this section, we try to see what is happening here and how we might predict the minimal number of squares required to represent a given positive integer.

As usual, we begin by restricting ourselves to primes and since the squares modulo 4 are $0, 1$, we immediately see that a prime congruent to 3 mod 4 is NOT the sum of two squares, (this is, of course, true for any integer n, not just primes), while the situation for primes congruent to 1 mod 4 is covered by the following theorem:

Theorem 1.7: Suppose p is a prime congruent to 1 mod 4. Then p can be expressed as the sum of two integer squares.

Proof: By the corollary to Wilson's Theorem, there is an $x \in \mathbb{Z}_p$ such that $x^2 \equiv -1 \mod p$. Consider the set $S = \{0, 1, 2, ..., \lfloor \sqrt{p} \rfloor\}$ and all the numbers of the form $a + bx$ with $a, b \in S$.

There are $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ choices for the a and b, so, modulo p, by the pigeon-hole principle,

$$a + bx \equiv A + Bx \mod p$$

for some $a, b, A, B \in S$, and the pair $(a, b) \neq (A, B)$. Hence

$$(a - A) \equiv (B - b)x \mod p \Rightarrow (a - A)^2 \equiv -(B - b)^2 \mod p \Rightarrow (a - A)^2 + (B - b)^2 = cp$$

for some integer c. But $|a - A| < \sqrt{p}$ and $|b - B| < \sqrt{p}$, so $(a - A)^2 + (B - b)^2 < 2p$ which gives $c = 1$ and the result follows.

Note, of course, that $2 = 1^2 + 1^2$, so this deals with all the primes.

The simple identity, $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$, which shows that the product of two numbers, each of which is the sum of two squares, is also the sum of two squares, enables us, (with a little extra work), to conclude that:

Theorem 1.8: Factor the positive integer n as

$$n = 2^{\epsilon} n_1^2 p_1 p_2 ... p_k$$

where $\epsilon \in \{1, -1\}$ and p_i is a prime.

Then, n is the sum of two squares iff $p_i \equiv 1 \mod 4$ for $i = 1, 2, ..., k$.

(Note that writing $(a^2 + b^2) = |a + ib|^2 = N(a + ib)$ proves the identity and gives us a simple way to produce a desired representation.)

Example: $n = 5525 = 5^2 \times 13 \times 17$.

The Number of Representations:

We now know exactly which numbers can be represented by the sum of two squares and so we turn to the question of the **number** of a such representations. We will count a representation such as $5 = 2^2 + 1^2$ as having 8 representations, since we can write

$$5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2.$$

We will write $N(n)$ to denote the number of representations of n as a sum of two squares, counting sign and order, so by the above, $N(5) = 8$.

We introduce the function $f(n) = D_1(n) - D_3(n)$, where $D_i(n)$ denotes the number of divisors of n of the form $4k + i$.

The following theorem, (which we state without proof), goes back to Jacobi.

Theorem 1.9:

With the above notation, for any positive integer $n > 1$, we have

$$N(n) = 4f(n).$$

Thus, if $n = p$, a prime of the form $4k + 1$, then $N(p) = D_1(p) = 8$ and so, ignoring order and signs, there is only one way to express such a prime as a sum of two squares.

Pythagorean Triples:

Before looking at sums of 3 and 4 squares, we digress briefly to look at Pythagorean triples.

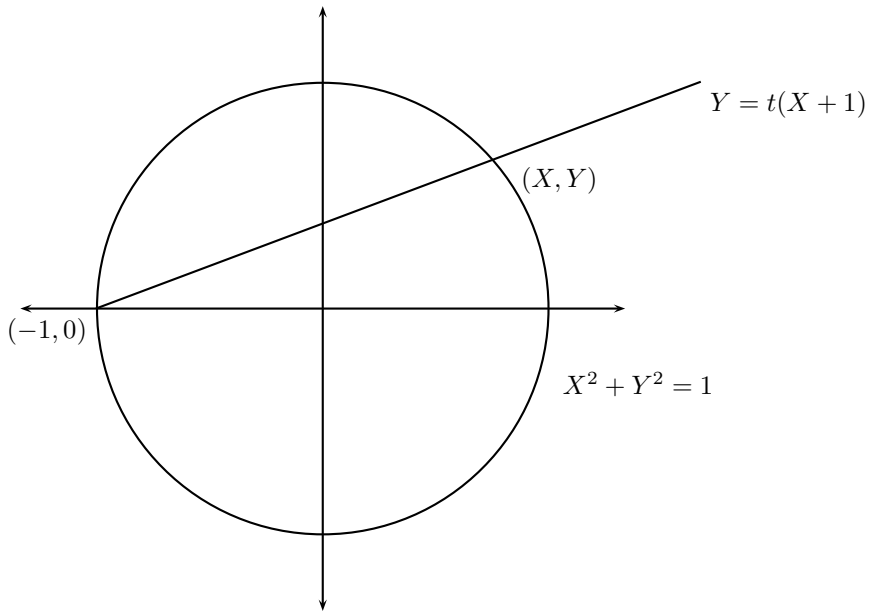
A triple (x, y, z) of positive integers such that $x^2 + y^2 = z^2$ is known as a **Pythagorean Triple.**

We wish to find all such triples.

Firstly, we take the equation $x^2 + y^2 = z^2$ and divide by z^2 to get $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$, so that if x, y, z are integers, then $\frac{x}{z}$ and $\frac{y}{z}$ are **rational** numbers. Put $X = \frac{x}{z}, Y = \frac{y}{z}$.

So, given integers x, y, z such that $x^2 + y^2 = z^2$, the equation $X^2 + Y^2 = 1$ has rational solutions, and conversely, if we can find rational solutions of $X^2 + Y^2 = 1$, we can express X and Y with a same denominator and thus get integers x, y, z with $x^2 + y^2 = z^2$.

Hence the problem of finding triads is equivalent to finding **rational** points on the circle $X^2 + Y^2 = 1$. (Note that the correspondence is NOT 1-1, since we can get $(3, 4, 5)$ and $(6, 8, 10)$ etc. from the same rational point $(\frac{3}{5}, \frac{4}{5})$. If however, we insist that $\gcd(x, y, z) = 1$ then the correspondence is 1-1.)



Consider the circle $X^2 + Y^2 = 1$ and draw a line passing through the point $(-1, 0)$ with slope t, which meets the circle at a point (X, Y). We restrict t between 0 and 1 so there will be an intersection point in the first

quadrant.

The equation of the line is $Y = t(X + 1)$.

Now observe that if (X, Y) is a rational point, then $t = \frac{Y}{X+1}$ is also rational. Conversely, if t is rational, solving the line $Y = t(X + 1)$ with the circle $X^2 + Y^2 = 1$, we have

$$(1 + t^2)X^2 + 2t^2X + (t^2 - 1) = 0.$$

We know that one of the roots is $X = -1$, so the other root is $X = \frac{1-t^2}{1+t^2}$ and so $Y = \frac{2t}{1+t^2}$. Thus, if t is rational, $(0 < t < 1)$, then (X, Y) will also be rational.

Example: $t = \frac{73}{91}$ gives $(X, Y) = (\frac{2952}{13610}, \frac{13286}{13610})$, hence $(2952, 13286, 13610)$ is a pythagorean triad.

We can now construct formulae to generate all the triads.

Put $t = \frac{u}{v}$, so $X = \frac{v^2-u^2}{v^2+u^2}, Y = \frac{2uv}{v^2+u^2}$. Thus

$$x = k(v^2 - u^2), \quad y = 2uvk, \quad z = k(u^2 + v^2)$$

where k is an integer, and $0 < u < v$.

Example: $k = 1, u = 5, v = 7$; gives the triad $(24, 70, 74)$

Note that the k is important if all triads are to be obtained. For example, if $k = 1$, the triad $(9, 12, 15)$ cannot be obtained.

Primitive triads:
If (a, b, c) is a triad and $\gcd(a, b, c) = 1$ then the triad is said to be *primitive*. A little thought will reveal that the conditions required on u, v and k to generate primitive triads are:

$k = 1$, $\gcd(u, v) = 1$ **and** u and v have opposite parity.

Example: $u = 5, v = 7$ does not yield a primitive triad (as seen in the above example) since the numbers are both odd.

$u = 2, v = 3$ gives the triad $(5, 12, 13)$ which is clearly primitive.

An Application to Fermat's Last Theorem for $n = 4$.

Fermat claimed that the equation $x^n + y^n = z^n$ has no positive integer solutions (x, y, z) for $n \geq 3$. He also claimed to have a proof, but never wrote it down. This result has only recently been proven using very advanced techniques. The problem is generally refered to as 'Fermat's Last Theorem' and was one of the 'holy grails' of mathematics.

We can use the ideas developed above to prove it true for the case $n = 4$.

Firstly note that if $x^4 + y^4 = z^4$ has integer solutions then so does $x^4 + y^4 = z^2$, so suppose (x, y, z) satisfy this last equation with z **as small as possible**. The idea is to find integers (X, Y, Z) such that $X^4 + Y^4 = Z^2$, with $Z < z$, thus contradicting the minimality of z.

(This technique is known as the "Method of Infinite Descent" and seems to have been first used by Fermat.)

We may suppose that x, y, z have no common factor and that $\gcd(x, y) = 1$. Therefore (x^2, y^2, z) forms a primitive pythagorean triad, and so $x^2 = p^2 - q^2, y^2 = 2pq, z = p^2 + q^2$, where p, q are relatively prime integers with opposite parity.

Now if p is even, q odd, then $x^2 \equiv 3 \bmod 4$ which is impossible, so p is odd and q even. Put $q = 2r$ giving

$$x^2 = p^2 - (2r)^2, \left(\frac{1}{2}y\right)^2 = pr \text{ with gcd } (p, r) = 1$$

The second of these equations implies that p and r are perfect squares, so put $p = Z^2, r = W^2$, hence

$$x^2 + (2W^2)^2 = Z^4$$

so $(x, 2W^2, Z^2)$ is a primitive triad, and thus we can write

$$x = P^2 - Q^2, 2W^2 = 2PQ, Z^2 = P^2 + Q^2 \text{ with } \gcd(P, Q) = 1.$$

(Check here that $2W^2 = P^2 - Q^2$ is not possible, since P and Q must have opposite parity.)

The second equation again gives P, Q squares, so put $X^2 = P, Y^2 = Q$, then from the third equation we have $X^4 + Y^4 = Z^2$ but

$Z^2 = p = \sqrt{z - q^2} < \sqrt{z} < z < z^2$, so $Z < z$, contradicting the minimality of z.

Sums of Three Squares:

We have seen that certain numbers cannot be written as the sum of two squares, and there are numbers, such as 15, which cannot be written as the sum of three squares. We would like to characterise when a number can be written as the sum of three squares.

Lemma: If $x \equiv 7 \bmod 8$ then x cannot be written as the sum of three squares.

Proof:

The full story is:

Theorem 1.10: An integer n can be expressed as the sum of (at most) three integer squares unless $n = 4^\alpha(8k + 7)$, for some integers α and k.

Proof:

Sums of Four Squares:

The following theorem, due to Lagrange, completes the story on sums of squares. We will not give the proof here, but it can be gotten from an interesting generalisation of complex numbers called quaternions, from which the following (amazing!) identity is derived.

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = (ax+by+cz+dw)^2 + (ay-bx-cw+dz)^2$$

$$+(az+bw-cx-dy)^2 + (aw-bz+cy-dx)^2.$$

This tells us that if X and Y are the sum of four squares, then so is their product. From this, one can (with a lot of work!) prove:

Theorem 1.11: (Lagrange) Every integer can be expressed as the sum of (at most) four squares.

Proof: Deleted.

Waring's Problem:

Having dealt with representations by sums of squares, it is natural to ask about higher powers. For example, it is known that every integer can be written as the sum of (at most) nine cubes. In fact only the numbers 23 and 239 actually require nine cubes,viz. $23 = 2^3+2^3+1^3+1^3+1^3+1^3+1^3+1^3+1^3$.

In 1970 it was shown that every integer can be written as the sum of 19 fourth powers.

For each positive integer k, let $G(k)$ be the minimum number of kth powers required to represent every integer, equivalently, we want the smallest number $G(k)$, such that $x = x_1^k + x_2^k + ... + x_{G(k)}^k$ has integer solutions $x_1, ..., x_{G(k)}$, for all integers x.

Can we find a formula for $G(k)$? No such formula is known and the problem is often refered to as Waring's problem.

It is known that:

$G(2) = 4$ (Theorem 1.11)
$G(3) = 9$
$G(4) = 19$
$G(5) = 37.$

As we have seen, for fixed k only certain numbers actually need $G(k)$ terms, for example with $k=3$, only 23 and 239 need nine cubes.

Consider the number $n = 2^k\left[\left(\frac{3}{2}\right)^k\right] - 1$, where $[x]$ denotes the greatest integer less or equal to x. Observe that if $k=3, n=23$. This number n then, is an attempt to find the 'worst' case for each k.

Also note that $n < 2^k\left(\frac{3}{2}\right)^k - 1 < 2^k.\frac{3^k}{2^k} = 3^k$, so to represent n as the sum of kth powers, we need $x_i < 3$, i.e. $x_i \leq 2$. In fact we need $\left(\left[(\frac{3}{2})^k\right] - 1\right)$ lots of 2^k, leaving (2^k-1) lots of 1^k.

That is, we can write n as

$$n = \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right).\underline{2^k} + (2^k-1).\underline{1^k}$$

This would require $\left[\left(\frac{3}{2}\right)^k\right] - 1 + 2^k - 1 = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$ terms, so

$$G(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$$

which we will call $l(k)$.

Observe that

$$l(2) = 4 = G(2)$$
$$l(3) = 9 = G(3)$$
$$l(4) = 19 = G(4)$$
$$l(5) = 37 = G(5)$$

It is believed that $G(k) = l(k)$ but no proof has been found.