Week 2: Number Theory - Sum of Squares and Vieta Jumping

1 Primes 1 and 3 (mod 4)

The following is an important fact distinguishing primes that are $1 \pmod 4$ and those that are $3 \pmod 4$.

Theorem 1.1 *Let p be a prime. Then $x^2 \equiv -1 \pmod p$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof: If $p \equiv 1 \pmod 4$, then let $p = 4k + 1$. We leave to the reader to prove that $(2k!)^2 \equiv -1 \pmod p$.

If $p = 2$, clearly $x = 1$ is a solution. If $p \equiv 3 \pmod 4$, then suppose $x^2 \equiv -1 \pmod p$. Let $p = 4k + 3$. Then by Fermat's Little Theorem, $x^{4k+2} \equiv 1 \pmod p$. Since $x^2 \equiv -1 \pmod p$, $x^{4k+2} \equiv -1 \pmod p$. Hence, $1 \equiv -1 \pmod p$, implying that $p = 2$. Hence, $p \not\equiv 3 \pmod 4$. This is a contradiction. Therefore, $x^2 \equiv -1 \pmod p$ has no integer solutions if $p \equiv 3 \pmod 4$. $\square$

Corollary 1.2 *Let n be a positive integer. Then n^2+1 is not divisible by 4 and not divisible by any prime which is $3 \pmod 4$.*

Example 1.3 *Prove that there are no positive integer solutions to $4ab - a - b = c^2$.*

Proof: Suppose a positive integer solution to this equation exists. We can rewrite this equation as $16 - 4a - 4b + 1 = 4c^2 + 1$, or equivalently,

$$(4a - 1)(4b - 1) = 4c^2 + 1.$$

Since $a, b \geq 1$, $(4a-1)(4b-1)$ contains a prime factor congruent to $3 \pmod 4$. But $4c^2+1$ cannot have this property. This is a contradiction. $\square$

Exercise:

1. Find all positive integer solutions (x, y) such that $x^2 = y^3 + 23$.

2. Prove that $n^7 + 7$ is not a perfect square for any positive integer n.

3. (IMO 2008) Prove that there are infinitely many positive integers n such that $n^2 + 1$ has a prime divisor greater than $2n + \sqrt{2n}$.

2 Sum of Squares

The goals of this section are:
• to demonstrate the Brahmagupta-Fibonacci identity
• to determine which integers can be written as the sum of two perfect squares

We first present the BrahmaguptaFibonacci identity.

Theorem 2.1

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

It is important to note that this identity can be written in two different ways, i.e.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

This might come in handy. (*cough* Upcoming Exercise 1 *cough*)

Let

$$\mathcal{S} = \{a^2 + b^2 \quad | \quad a, b \in \mathbb{Z}\}.$$

Theorem 2.2

1. *Let p be a prime number. Then $p \in \mathcal{S}$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

2. *Use the Brahmagupta-Fibonacci identity, prove that if $m, n \in \mathcal{S}$, then $mn \in \mathcal{S}$.*

3. *Let p be a prime in $\mathcal{S}$. Prove that $m \in \mathcal{S}$ if and only if $pm \in \mathcal{S}$.*

Proof: Since $x^2 \equiv 0, 1 \pmod 4$ for every integer n, $x^2 + y^2 \not\equiv 3 \pmod 4$. Therefore, if $p \equiv 3 \pmod 4$, $p \notin \mathcal{S}$. If $p = 2$, then clearly $2 \in \mathcal{S}$ since $2 = 1^2 + 1^2$. If $p \equiv 1 \pmod 4$, then there exists a positive integer a such that $a^2 \equiv -1 \pmod 4$. Consider all integers of the form $ax - y$, where x, y are integers such that $0 \leq x, y < \sqrt{p}$. The number

of pair of positive integers (x, y) is then $(\lfloor\sqrt{p}\rfloor + 1)^2 > (\sqrt{p})^2 = p$. By Pigeonhole Principle, there exists integers $(x_1, y_1) \neq (x_2, y_2)$ such that $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$. Then $a(x_1 - x_2) \equiv (y_1 - y_2) \pmod{p}$. Since $a^2 \equiv -1 \pmod{p}$,

$$-(x_1 - x_2)^2 \equiv (y_1 - y_2)^2 \pmod{p}.$$

Then $(x_1 - x_2)^2 + (y_1 - y_2)^2$ is divisible by p. Then $0 < (x_1 - x_2)^2 + (y_1 - y_2)^2 < 2p$. Then $(x_1 - x_2)^2 + (y_1 - y_2)^2 = p$. This proves (1).

(2) follows immediately from the BrahmaguptaFibonacci identity.

To prove (3), let $p = u^2 + v^2$ and $pm = x^2 + y^2$. Then $m = \frac{x^2+y^2}{u^2+v^2}$. But since

$$(ux + vy)^2 + (uy - vu)^2 = (u^2 + v^2)(x^2 + y^2).$$

Then we get that

$$\left(\frac{ux + vy}{u^2 + v^2}\right)^2 + \left(\frac{uy - vx}{u^2 + v^2}\right)^2 = \frac{x^2 + y^2}{u^2 + v^2}$$

and

$$\left(\frac{uy + vx}{u^2 + v^2}\right)^2 + \left(\frac{ux - vy}{u^2 + v^2}\right)^2 = \frac{x^2 + y^2}{u^2 + v^2}.$$

It now suffices to show that $p|ux - vy$ or $p|ux + vy$. Since this would imply that the terms inside the brackets for at least one of the two equations are all integers. This fact is clear since $(ux-vy)(ux+vy) = u^2x^2-v^2y^2 \equiv u^2x^2-(-u^2)(-x^2) \equiv 0 \bmod p$. Therefore, $p|ux-vy$ or $p|ux + vy$. $\square$

Exercise

1. Prove that the n is the sum of two perfect squares if and only if every prime $p \equiv 3 \pmod{4}$ divides n an even number of times. (Hint: Use the previous theorem.)

2. Let n be a positive integer that can be written as the sum of two perfect squares in two different ways. Prove that n is composite.

3. Let f be a polynomial with real coefficients such that $f(x) \geq 0$ for all $x \in \mathbb{R}$. Prove that there exists $g, h \in \mathbb{R}[x]$ such that $f(x) = g(x)^2+h(x)^2$. (Hint: Factor f completely into polynomials with real coefficients. Each factor is either linear or quadratic. (Why?))

4. Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(ax + by) + f(ay - bx) = (f(a) + f(b))(f(x) + f(y))$$

for all $a, b, x, y \in \mathbb{R}$.

3 Vieta Jumping

Ah the infamous number theory solving technique. If you know of it, great! If not, here it is in its glory. It's probably best to do this with an example.

Exercise 3.1 *Let m, n be positive integers such that $m^2 + n^2$ is divisible by $mn + 1$. Prove that*

$$\frac{m^2 + n^2}{mn + 1}$$

is a perfect square.

Proof: Let

$$\mathcal{S} = \left\{ (m, n) \mid \frac{m^2 + n^2}{mn + 1} \text{ is an integer.} \right\}.$$

Note that $\mathcal{S}$ is symmetric, i.e. $(m, n) \in \mathcal{S}$ if and only if $(n, m) \in \mathcal{S}$. If $m = n$, then $2m^2$ is divisible by $m^2 + 1$. Since $2m^2/(m^2 + 1) < 2$, $2m^2 = m^2 + 1$. Hence, $m = n = 1$. Then $(m^2 + n^2)/(mn + 1)$ is a perfect square. We will now suppose that $m \neq n$.
Suppose

$$\frac{m^2 + n^2}{mn + 1} = k$$

for some positive integer k which is not a perfect square and (m, n) is chosen minimally. Rewriting this gives us

$$m^2 - kn \cdot m + (n^2 - k).$$

Then consider the quadratic equation $x^2 - knx + (n^2 - k) = 0$. Note that m is one root. Let m' be the other root. Since m is an integer, m' is also an integer. We have $m + m' = kn, mm' = n^2 - k$. WLOG, suppose $m > n$. Then since $mm' = n^2 - k$, $m' < m$. If $m' > 0$, then $(m', n) \in \mathcal{S}$, contradicting the minimality of (m, n). If $m' = 0$, then since $mm' = n^2 - k$, $n^2 = k$, a perfect square. This contradicts our assumption about k. If $m' < 0$, $(m' + 1)(m + 1) \leq 0 \Rightarrow kn + (n^2 - k) + 1 \leq 0 \Rightarrow k(n - 1) + n^2 + 1 \leq 0$. This is also a contradiction. Therefore, k is a perfect square.

The important ingredients of a Vieta jumping solution are
• Setting a set like $\mathcal{S}$ in this past exercise. Usually, $\mathcal{S}$ is **symmetric**

• Assume some minimality (or maximality) condition on $\mathcal{S}$.

• Root-flopping, i.e. if $(m, n) \in \mathcal{S}$ and $m > n$, then $(m', n) \in \mathcal{S}$ for some $m' < n$. Then $(n, m') \in \mathcal{S}$ and we repeat. The minimality condition on $\mathcal{S}$ will somehow be violated.

Note: Sometimes finding the quadratic equation for which to set up the Vieta jumping requires some work beforehand. Sometimes the quadratic equation is practically given to you. Please practice the following problems to become familiar with this powerful technique.

Exercises

1. Find all pairs of positive integers (a, b) such that
$$\frac{a^2 + b^2 + 1}{ab}$$
is an integer.

2. Find all pairs of positive (a, b) such that
$$a \mid b^2 + 1, b \mid a^2 + 1.$$

3. (Romania 2005) Find all quadruples of positive integers (a, b, m, n) such that
$$a^m b^n = (a + b)^2 + 1.$$

4. (IMO 2007) Let a, b be positive integers such that
$$4ab - 1 \mid (4a^2 - 1)^2.$$
Prove that $a = b$.

5. (Ireland 2005) Let m, n be integers with the same parity such that $m^2 - n^2 + 1$ divides $n^2 - 1$. Prove that $m^2 - n^2 + 1$ is a perfect square.

6. (IMO 1981) Find all pairs of positive integers (a, b) such that $1 \leq a, b \leq 1000$ and
$$(a^2 - ab - b^2)^2 = 1.$$