Number Theory - Quadratics

by Adrian Tang, tang@math.ucalgary.ca

1. Perfect squares mod n

We are interested in solving the following problem. Let n be a positive integer and a be an integer such that $0 \leq a < n$. Does there exists an integer x such that

$$x^2 \equiv a \bmod n.$$

For example, are there integers x such that $x^2 \equiv 0 \bmod 4$? $\equiv 1 \bmod 4$? $\equiv 2 \bmod 4$? $\equiv 3 \bmod 4$?

Naturally, for any integer b, there always exist an integer x such that $x^2 \equiv b^2 \bmod n$, namely $x = b$ or $x = -b$. Hence, there always exist an integer x such that $x^2 \equiv 0 \bmod n$ and an integer y such that $y^2 \equiv 1 \bmod n$ for any given n.

Exercise 1: Prove that every perfect square is congruent to either 0 or 1 mod 4. Prove that every perfect square is congruent either $0, 1$ or 4 mod 8.

Exercise 2: Prove that $x^2 + y^2 = 2007$ has no integer solutions. Prove that $x^2 + y^2 + z^2 = 2007^{2007}$ has no integer solutions.

This set of notes will focus strictly on quadratics. General diophantine equations will be handled in another set of notes.

The next goal is to find all prime numbers p such that $x^2 \equiv -1 \bmod p$ has an integer solution x. We will first recall Fermat's Little Theorem.

Fermat's Little Theorem Let p be a prime and a be a positive integer.
a.) If a is not divisible by p, then

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

b.) For all positive integers a,

$$a^p \equiv a \bmod p.$$

Proof: If a is not divisible by p, then $gcd(a, p) = 1$. Recall from basic modular arithmetic that $\{1, 2, \cdots, p-1\} = \{a, 2a, \cdots, (p-1)a\}$ modulo p as sets. Hence, the products of the elements of each set are equal, i.e.

$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \bmod p.$$

Cancelling both sides by $(p-1)!$ (which is allowed since $gcd((p-1)!, p) = 1$) yields the desired result for (a). The conclusion of (b) is yielded by multiplying both sides of (a) by a if $p \nmid a$ and the statement is clear if $p \mid a$. □

We are now ready to determine which prime p yields an integer solution for the equation $x^2 \equiv -1 \bmod p$.

Proposition: Let p be a prime. Then there exists an integer x such that

$$x^2 \equiv -1 \bmod p$$

if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

Proof: If $p = 2$, then set $x = 1$. If $p \equiv 1 \bmod 4$, let $p = 4k + 1$. We leave as an exercise to the reader to prove (using Wilson's Theorem) that $(2k)! \equiv -1 \bmod (4k + 1)$. If $p \equiv 3 \bmod 4$, let $p = 4k + 3$. Then $1 \equiv x^{p-1} \equiv x^{4k+2} \equiv (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \bmod p$, implying $p = 2$, contradiction. □

Now how does this help us? Observe that every integer n which is 3 mod 4 has a prime factor which is also 3 mod 4. This shows that every prime factor of an integer of the form $n^2 + 1$ is either 2 or congruent to 1 mod 4. We demonstrate this with an example.

Exercise 3: Prove that $y^2 = x^3 + 7$ has no integer solutions.

Solution: Note that x is odd, since if x is even, then $y^2 \equiv 3 \bmod 4$, which is impossible. If $x \equiv 3 \bmod 4$, then $y^2 \equiv 2 \bmod 4$, which is also impossible. Hence, $x \equiv 1 \bmod 4$. Then this can be re-written as

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4).$$

Since $x + 2 \equiv 3 \bmod 4$, this implies $y^2 + 1$ has a factor which is congruent to 3 mod 4, and this factor must contain a prime factor which is 3 mod 4, impossible. Therefore, this equation has no integer solutions. □

Related Exercises:

1. Prove that $y^2 = x^3 + 23$ has no integer solutions.
2. Prove that $4ab + a + b = c^2$ has no positive integer solutions.

We now explore which primes p has the property that there exists an integer x such that $x^2 \equiv 2 \bmod p$. Clearly, $p = 2$ yields a solution. Now, let's move on to odd primes p.

Proposition: Let p be an odd prime. Then there exists an integer x such that

$$x^2 \equiv 2 \bmod p$$

if and only if $p \equiv 1, -1 \bmod 8$.

Proof: Postponed. Hint: Simplify $2^{\frac{p-1}{2}}(\frac{p-1}{2})!$. □

Specifically, if $p \equiv \pm 3 \bmod 8$, then $x^2 \equiv 2 \bmod p$ yields no solutions.

Related Exercises

1. Let p be an odd prime. Prove that there exists an integer n such that $n^8 - 16$ is divisible by p.

2. Let p be an odd prime which is at least 5. Let m, n be relatively prime positive integers such that

$$\frac{m}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

Prove that m is divisible by p^2.

2. Sum Of Two Squares

The goal of this section to characterize all positive integers that can be written as the sum of two perfect squares. On the way to proving this characterization, the notes will provide exercises that requires useful techniques in solving number theory problems in general. The proof of this characterization is not easy. I will break this down into several number theory exercises. For the remaining of this set of notes, I will use the following notation.

$$\mathcal{S} = \{n \in \mathbb{Z} | a^2 + b^2 = n \text{ for some } a, b \in \mathbb{Z}\ \}$$

Clearly, perfect squares themselves are in S, since they are the sum of themself and zero, which is a perfect square. There is a class of integers which is certainly not in S.

Exercise 1: Prove that if $n \equiv 3 \bmod 4$, then $n \notin \mathcal{S}$.

Solution: First, you want to prove that $x^2 \equiv 0$ or $1 \bmod 4$ for all integers x. Since $x^2 \equiv 0, 1 \bmod 4$ for all integers x, then $x^2 + y^2 \not\equiv 3 \bmod 4$. □

We next examine the integers that are in S. We will soon show that S is closed under multiplication, i.e. if $a, b \in S$ then $ab \in S$. We will start with a specific example of this claim.

Exercise 2: Let n be a positive integer. Prove that $n \in \mathcal{S}$ if and only if $2n \in \mathcal{S}$.

Solution: Suppose $n = x^2 + y^2$. Then $2n = (x + y)^2 + (x - y)^2$. Conversely if $2n = a^2 + b^2$, then $a \equiv b \bmod 2$. Therefore, $(a + b)/2, (a - b)/2 \in \mathbb{Z}$. Then $n = ((a + b)/2)^2 + ((a - b)/2))^2$. □

We will now generalize Exercise 2.

Exercise 3: Prove that if $m, n \in \mathcal{S}$, then $mn \in \mathcal{S}$.

Solution: Let $m = a^2 + b^2, n = u^2 + v^2$. Then $mn = (a^2 + b^2)(u^2 + v^2) = a^2u^2 + b^2v^2 + a^2v^2 + b^2u^2 = (au + bv)^2 + (av - bu)^2$, as desired. □

We have now established an extremely important identity in number theory.

Brahmagupta-Fibonacci Identity: Let $a, b, c, d \in \mathbb{Z}$. Then

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

Note that this can be expressed in a second way.

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

The fact that the product of two numbers in $\mathcal{S}$, can be written as the sum of squares in essentially two different ways. This fact may come in handy.

Exercise 4: Let p be a prime in $\mathcal{S}$. Prove that $m \in \mathcal{S}$ if and only if $pm \in \mathcal{S}$.

Solution: The direction ($\Rightarrow$) is clear from Exercise 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

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

and

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

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 $p|ux + vy$. □

Exercise 5: Suppose $n \in \mathcal{S}$ contains a factor $m \notin \mathcal{S}$. Prove that n/m also contains a factor not in $\mathcal{S}$.

Solution: Let $n/m = p_1p_2 \cdots p_t$ be the prime factorization of n/m. If any p_i is not in $\mathcal{S}$, we are done. Otherwise, suppose $p_i \in \mathcal{S}$ for all i. Then by Exercise 4, $n/(p_1p_2 \cdots p_t) \in \mathcal{S} \Rightarrow m \in \mathcal{S}$, contradiction. □

Exercise 6: Prove that if a, b are positive integers such that $gcd(a, b) = 1$, then every factor of $a^2 + b^2 \in \mathcal{S}$.

Solution: Suppose that $a^2 + b^2$ contains a factor $x \notin \mathcal{S}$. We choose (a, b) subject to the condition and that $gcd(a, b) = 1$ and the factor x is minimized. (*)

Let $a = mx + n, b = ux + v$ such that $|n|, |v| \leq x/2$. Then $x|a^2 + b^2 \Rightarrow x|(mx + n)^2 + (ux + v)^2 \Rightarrow x|n^2 + v^2$. Let $n^2 + v^2 = xz$. By the bounds on n, v, we know that $z \leq x/2$.

Let $d = gcd(n, v)$. Therefore $d^2|xz$. Since $gcd(d, x)|a, b$, then $gcd(d, x) = 1$ since a, b are relatively prime. Hence, $d^2|z$. We now have

$$(\frac{n}{d})^2 + (\frac{v}{d})^2 = x \cdot \frac{z}{d^2}.$$

Let $a' = \frac{n}{d}, b' = \frac{v}{d}$. Then $gcd(a', b') = 1$ and since $x \notin \mathcal{S}$, $\frac{z}{d^2} = (a'^2 + b'^2)/x$ contains a factor not in $\mathcal{S}$ (by Exercise 5) but is smaller than $x/2$, which is smaller than x. This is also a factor of $a'^2 + b'^2$. This contradicts the minimality of x subject to condition (*). □

Exercise 7: Prove that every prime that is either 2 or congruent to 1 mod 4 is in $\mathcal{S}$.

Clearly, $2 \in \mathcal{S}$. Let $p \equiv 1 \bmod 4$. Let $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod p$. (A solution for this always exist for $p \equiv 1 \bmod 4$) Then $p|a^2 + 1$. By Exercise 6, $p \in \mathcal{S}$. □

Exercise 8: In terms of prime factorization, characterize all integers in $\mathcal{S}$.

Any integer n such that each prime factor p of n which is 3 mod 4 appears an even number of times in the prime factorization of n is in $\mathcal{S}$, by Exercises 3 and 8. Conversely, suppose $p \equiv 3 \bmod 4$, and e is odd and is the highest power of p dividing n. Then $a^2 + b^2 \equiv 0 \bmod p \Rightarrow a^2 \equiv -b^2 \bmod p$. Since -1 is not a square mod

p (since $p \equiv 3 \bmod 4$), then $a, b \equiv 0 \bmod p$, then the highest power of p dividing $(a/p)^2 + (b/p)^2$ is $e-2$. Repeating this process, we get integers a', b' such that $a'^2 + b'^2$ is divisible by p but not p^2, which is impossible. □

We summarize these results as follows;

Integers Expressible as the Sum of Two Squares: An integer n is expressible as the sum of two perfect squares if and only if for every prime $p \equiv 3 \bmod 4$, p divides n an even number of times.

Exercises:

1. Let n be a positive integer that can be written as the sum of two squares in two different ways (up to order). Prove that n is composite.

2. Let a, b, c be three positive integers such that $gcd(a, b, c) = 1$ and $a^2 + b^2 = c^2$.

   a.) Prove that one of a, b is odd, and the other of a, b is even. Prove also that c is odd.

   b.) Suppose a is odd and b is even. Prove that there exists positive integers m, n such that $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$.

3. Let f be a polynomial such that $f(x) \geq 0$ for all $x \in \mathbb{R}$. Prove that there exist polynomials $g(x), h(x) \in \mathbb{R}[x]$ such that
$$f(x) = g(x)^2 + h(x)^2.$$

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. Descent Methods in Solving Diophantine Equations

The main idea behind the descent method of solving diophantine equations is the following; say you are given a diophantine equation in two variables a, b. Suppose it contains a positive integer solution (a, b). We assume that (a, b) is a minimal solution. i.e. (a', b') is another positive integer solution with $a' \leq a, b \leq b'$ then $a = a', b = b'$. We begin with a simple example.

Exercise 1: Find all positive integer solutions to $a^2 = 2b^2$.

Solution: Suppose (a, b) is a positive integer solution. Note that a is even, which in fact implies that b is even. Suppose (a, b) is a minimal solution. Then note that $(a/2, b/2)$ is also another positive solution to this equation, contradicting the minimality of (a, b). Hence, this equation has no positive integer solutions. □

We will now show a more advanced descent method. It is based on the following basic fact about quadratic equation; let a, b be integers. Suppose the quadratic equation $x^2 + ax + b$ has one integer root. Then the other root is also an integer. This is clear since the two roots sum to $-a$, which is an integer. This technique is best demonstrated with an example.

Exercise 2: Let k be a positive integer of the form

$$k = \frac{a^2+b^2}{ab+1}$$

where a, b are positive integers. Prove that k is a perfect square.

Solution: Since the equation is symmetric about a and b we may assume that $a \geq b$. Let

$$S = \{(a,b)|\frac{a^2+b^2}{ab+1} = k\}$$

Suppose (a,b) is a minimal solution in S. We can rewrite this as $a^2+b^2 = k(ab+1)$. This equation is nice and quadratic. So let's write it as a quadratic with variable a, i.e. $a^2 - kba + b^2 - k = 0$. Consider the quadratic equation

$$x^2 - kbx + (b^2 - k) = 0.$$

One root of this equation is a. Let a' be the other root. Since $aa' = b^2 - k$ and $a \geq b$, then $a' < b < a$. If $a' > 0$, then note that (a', b) is also a solution in S, contradicting the minimality of (a,b). If $a' < 0$. Hence, $0 \geq (a'+1)(a+1) = aa' + a + a' + 1 = b^2 - k + kb + 1 > 0$, contradiction. Therefore, $a' = 0$. Since $aa' = b^2 - k$, then $k = b^2$, which is a perfect square. $\square$

This is an incredible solution for a problem at IMO 1988. The student that came up with this solution won a special prize for using such an ingenious idea! This notion of using the second root of a quadratic equation is common called *root-flipping* or *Vieta-jumping*. You have just learned a very special technique. It is time to practice it.

Exercises

1. Prove that $(36a+b)(36b+a)$ is not a power of 2 for any positive integer a, b.
2. Let a, b, k be positive integers such that
$$k = \frac{a^2+b^2}{ab-1}.$$
Prove that $k = 5$.
3. Find all positive integers that can be expressed in the form
$$\frac{a^2+b^2+1}{ab}$$
where a, b are positive integers.
4. Let a, b be positive integers such that $4ab-1$ divides $4a^2-1$. Prove that $a = b$.
5. Find all pairs of positive integers (m,n) such that $m|n^2+1$ and $n|m^2+1$.
6. Prove that there are infinitely many pairs of positive integers (a,b) such that $gcd(a,b) = 1$, $b|a^2-5$ and $a|b^2-5$.