An Application of Quotient Rings to Number Theory

William M. Faucette

Department of Computing and Mathematics
University of West Georgia

Student-Centered Seminar

Outline

The Problem

Some odd prime numbers p can be written as the sum of two squares of natural numbers.

Examples:

1. $1^2 + 2^2 = 5$
2. $1^2 + 4^2 = 17$
3. $4^2 + 5^2 = 41$
4. $5^2 + 6^2 = 61$
5. $22^2 + 23^2 = 1013$

The Problem

Some odd prime numbers p can be written as the sum of two squares of natural numbers.

Examples:

1. $1^2 + 2^2 = 5$
2. $1^2 + 4^2 = 17$
3. $4^2 + 5^2 = 41$
4. $5^2 + 6^2 = 61$
5. $22^2 + 23^2 = 1013$

The Problem

Some odd prime numbers p cannot be written as the sum of two squares of natural numbers.

Examples: The odd primes 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 cannot be written as the sum of two squares of natural numbers. (Proof shortly.)

The Problem

Some odd prime numbers p cannot be written as the sum of two squares of natural numbers.

Examples: The odd primes 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 cannot be written as the sum of two squares of natural numbers. (Proof shortly.)

The Problem

Some odd prime numbers are congruent to 1 modulo 4.

Examples:

$$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$$

The other odd prime numbers must be congruent to 3 mod 4.

Examples:

$$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83$$

The Problem

Some odd prime numbers are congruent to 1 modulo 4.

Examples:

$$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$$

The other odd prime numbers must be congruent to 3 mod 4.

Examples:

$$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83$$

The Problem

For some odd primes p, the equation $x^2 + 1 = 0$ has a solution modulo p. For other odd primes, the equation $x^2 + 1 = 0$ has no solution modulo p.

Examples:

1. $p = 3$: There is no solution, which can be checked by plugging in 0, 1, 2 modulo 3.
2. $p = 5$: For $x = 2$, we have $x^2 + 1 = 5 \equiv 0 \mod 5$.
3. $p = 7$: There is no solution, which can be checked by plugging in $0, \ldots, 6$ modulo 7.
4. $p = 37$: For $x = 31$, we have $x^2 + 1 = 962 \equiv 0 \mod 37$.

The Problem

For some odd primes p, the equation $x^2 + 1 = 0$ has a solution modulo p. For other odd primes, the equation $x^2 + 1 = 0$ has no solution modulo p.

Examples:

1. $p = 3$: There is no solution, which can be checked by plugging in 0, 1, 2 modulo 3.
2. $p = 5$: For $x = 2$, we have $x^2 + 1 = 5 \equiv 0 \mod 5$.
3. $p = 7$: There is no solution, which can be checked by plugging in $0, \ldots, 6$ modulo 7.
4. $p = 37$: For $x = 31$, we have $x^2 + 1 = 962 \equiv 0 \mod 37$.

The Conjecture

We have the following conjecture...

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that* $p = a^2 + b^2$.
2. *p is congruent to 1 modulo 4*
3. *The polynomial* $x^2 + 1$ *has a root in the integers modulo p.*

The Conjecture

We have the following conjecture...

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that* $p = a^2 + b^2$.
2. *p is congruent to 1 modulo 4*
3. *The polynomial* $x^2 + 1$ *has a root in the integers modulo p.*

The Conjecture

We have the following conjecture...

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that* $p = a^2 + b^2$.
2. *p is congruent to 1 modulo 4*
3. *The polynomial* $x^2 + 1$ *has a root in the integers modulo p.*

The Conjecture

We have the following conjecture...

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that* $p = a^2 + b^2$.
2. *p is congruent to 1 modulo 4*
3. *The polynomial* $x^2 + 1$ *has a root in the integers modulo p.*

The proofs of the first two steps here are very basic.

The proof that (3) implies (1) will use some basic results from abstract algebra, including a truly interesting application of quotient rings.

(1) implies (2):

First, we will show that (1) implies (2):

Theorem

If p is an odd prime number that can be written as $p = a^2 + b^2$ for some natural numbers a and b, then p must be congruent to 1 modulo 4.

Proof.

Let's look at squares modulo 4:

- $0^2 = 0$
- $1^2 = 1$
- $2^2 = 4 \equiv 0 \mod 4$
- $3^2 = 9 \equiv 1 \mod 4$

So, the only squares modulo 4 are 0 and 1.
Further, any odd number squared is congruent to 1 modulo 4, while any even number squared is congruent to 0 modulo 4. □

Proof.

Let's look at squares modulo 4:

- $0^2 = 0$
- $1^2 = 1$
- $2^2 = 4 \equiv 0 \mod 4$
- $3^2 = 9 \equiv 1 \mod 4$

So, the only squares modulo 4 are 0 and 1.
Further, any odd number squared is congruent to 1 modulo 4, while any even number squared is congruent to 0 modulo 4. □

Proof.

Suppose p can be written as the sum of two squares:

$$p = a^2 + b^2.$$

Since p is odd, one of a or b is even and the other is odd. It follows that one of a^2 or b^2 is congruent to 0 modulo 4 and the other is congruent to 1 modulo 4. Hence

$$p = a^2 + b^2 \equiv 1 \mod 4.$$

This shows (1) implies (2).

(2) implies (3):

Next, we will show that (2) implies (3):

Theorem

If p is an odd prime number that is congruent to 1 modulo 4, the equation

$$x^2 + 1 = 0$$

has an integral solution modulo p.

In order to prove this theorem, we need a result from number theory:

Theorem (Wilson's Theorem)

If p is a prime number, then

$$(p-1)! \equiv -1 \mod p$$

Remark: For $p = 2$, this theorem is trivial, so we only prove the result for p odd.

Proof: (of Wilson's Theorem).

Let p be an odd integer. The integers modulo p form a field, so every element of the set

$$\{1, \ldots, p-1\}$$

has a multiplicative inverse modulo p.

In any field, there are only two elements that are their own inverses: 1 and $-1 \equiv p-1 \mod p$.

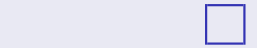
Proof: (of Wilson's Theorem).

Let p be an odd integer. The integers modulo p form a field, so every element of the set

$$\{1, \ldots, p-1\}$$

has a multiplicative inverse modulo p.

In any field, there are only two elements that are their own inverses: 1 and $-1 \equiv p-1 \mod p$.



Proof.

The remaining $p-3$ elements

$$\{2, \ldots, p-2\}$$

then can be grouped into pairs of numbers which are multiplicative inverses of each other. Hence, if we multiply all these numbers together, we get $1 \mod p$.

It follows that

$$\begin{aligned}(p-1)! &= (p-1)(p-2)(p-3)\cdots 3 \cdot 2 \cdot 1 \\ &\equiv -1 \cdot 1 \cdot 1 \\ &= -1 \mod p.\end{aligned}$$

Proof.

The remaining $p-3$ elements

$$\{2, \ldots, p-2\}$$

then can be grouped into pairs of numbers which are multiplicative inverses of each other. Hence, if we multiply all these numbers together, we get $1 \mod p$.

It follows that

$$\begin{aligned}(p-1)! &= (p-1)(p-2)(p-3)\cdots 3 \cdot 2 \cdot 1 \\ &\equiv -1 \cdot 1 \cdot 1 \\ &= -1 \mod p.\end{aligned}$$

Proof: (of (2) $\Rightarrow$ (3)).

Suppose p is a prime number congruent to 1 modulo 4. We want to find a solution of the equation

$$x^2 + 1 \equiv 0 \mod p.$$

Let

$$x = (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right).$$

Notice that since $p \equiv 1 \mod 4$, this product contains an even number of factors. □

Proof: (of (2) $\Rightarrow$ (3)).

Suppose p is a prime number congruent to 1 modulo 4. We want to find a solution of the equation

$$x^2 + 1 \equiv 0 \mod p.$$

Let

$$x = (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right).$$

Notice that since $p \equiv 1 \mod 4$, this product contains an even number of factors. □

Proof: (of (2) $\Rightarrow$ (3)).

Suppose p is a prime number congruent to 1 modulo 4. We want to find a solution of the equation

$$x^2 + 1 \equiv 0 \mod p.$$

Let

$$x = (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right).$$

Notice that since $p \equiv 1 \mod 4$, this product contains an even number of factors. $\square$

Proof:

Reducing modulo p, we get

$$\begin{aligned} x &= (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right) \\ &\equiv (-1)(-2)(-3)\cdots\left[\frac{p+1}{2}-p\right] \\ &\equiv (-1)(-2)(-3)\cdots\left(-\frac{p-1}{2}\right) \\ &\equiv (1)(2)(3)\cdots\left(\frac{p-1}{2}\right), \end{aligned}$$

the last step being true because the product has an even number of factors. □

Proof.

Hence, we see that

$$\begin{aligned} x^2 &= x \cdot x \\ &= (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right)\cdot\left(\frac{p-1}{2}\right)\cdots(3)(2)(1) \\ &= (p-1)! \\ &\equiv -1 \mod p. \end{aligned}$$

Thus, this value of x solves the equation $x^2 + 1 \equiv 0$ modulo p. □

Example:

Take $p = 13$, which is congruent to 1 modulo 4.
Let

$$\begin{aligned} x &= (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right) \\ &= 12 \cdot 11 \cdot 10 \cdot \cdots \cdot 7 \\ &= 665280 \\ &\equiv 5 \mod 13. \end{aligned}$$

Then,

$$x^2 + 1 = 5^2 + 1 = 26 \equiv 0 \mod 13.$$

Example:

Take $p = 13$, which is congruent to 1 modulo 4.
Let

$$\begin{aligned} x &= (p-1)(p-2)(p-3)\cdots\left(\frac{p+1}{2}\right) \\ &= 12 \cdot 11 \cdot 10 \cdot \cdots \cdot 7 \\ &= 665280 \\ &\equiv 5 \mod 13. \end{aligned}$$

Then,

$$x^2 + 1 = 5^2 + 1 = 26 \equiv 0 \mod 13.$$

(3)⇒(1)

To finish proving our conjecture, we must show that (3) implies (1). This is the step where we make a creative use of abstract algebra.

Review of Rings

Recall from abstract algebra that a ring is a set with two operations satisfying a certain set of algebraic properties.

There are two rings I especially want you to recall:

First Example of a Ring

First, $\mathbb{Z}_p[x]$ is the ring of polynomials with coefficients in the integers modulo p:

$$\mathbb{Z}_p[x] := \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}_p \text{ for all } i\}$$

Second Example of a Ring

Second, $\mathbb{Z}[i]$, the ring of Gaussian integers, is defined as the subring of the complex numbers of the form

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}.$$

We also recall that both $\mathbb{Z}_p[x]$ and $\mathbb{Z}[i]$ are **principal ideal domains**. That is, they are **integral domains** (i.e., if $xy = 0$, then either $x = 0$ or $y = 0$) in which every ideal is **principal** (i.e. the set of all multiples of a fixed element of the ring).

In all principal ideal domains, every element can be uniquely factored into a product of **units** (elements in the ring with multiplicative inverses) and **irreducible elements** (elements which only factor trivially, such as prime numbers in the integers).

We also recall that both $\mathbb{Z}_p[x]$ and $\mathbb{Z}[i]$ are **principal ideal domains**. That is, they are **integral domains** (i.e., if $xy = 0$, then either $x = 0$ or $y = 0$) in which every ideal is **principal** (i.e. the set of all multiples of a fixed element of the ring).

In all principal ideal domains, every element can be uniquely factored into a product of **units** (elements in the ring with multiplicative inverses) and **irreducible elements** (elements which only factor trivially, such as prime numbers in the integers).

First Isomorphism Theorem

Recall this fundamental theorem from ring theory:

Theorem

If $\phi : R \to S$ is a surjective homomorphism of rings with kernel I, then the map ϕ induces a quotient map

$$\overline{\phi} : R/I \to S,$$

which is an isomorphism. So, $R/I \cong S$.

First Example:

The natural quotient map

$$\phi : \mathbb{Z} \to \mathbb{Z}_p$$

extends to a surjective homomorphism on polynomial rings

$$\overline{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x].$$

The kernel of this map is the ideal (p) generated by the prime p, so

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x].$$

First Example:

The natural quotient map

$$\phi : \mathbb{Z} \to \mathbb{Z}_p$$

extends to a surjective homomorphism on polynomial rings

$$\overline{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x].$$

The kernel of this map is the ideal (p) generated by the prime p, so

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x].$$

Second Example:

The evaluation homomorphism

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$$

is defined by sending a polynomial $p \in \mathbb{Z}[x]$ to its value $p(i)$ at i.

This is a surjective ring homomorphism with kernel $(x^2 + 1)$, the ideal of all multiples of the polynomial $x^2 + 1$, so

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i].$$

Second Example:

The evaluation homomorphism

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$$

is defined by sending a polynomial $p \in \mathbb{Z}[x]$ to its value $p(i)$ at i.

This is a surjective ring homomorphism with kernel $(x^2 + 1)$, the ideal of all multiples of the polynomial $x^2 + 1$, so

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i].$$

A Truly Abstract Application

Let f and g be two elements in a commutative ring R. Let (f), (g), (f, g) be the ideals generated by those elements.

The homomorphism $\phi : R/(f) \to R/(f, g)$ is surjective with kernel (g), so

$$(R/(f))/(g) \cong R/(f, g).$$

A Truly Abstract Application

Similarly, we have

The homomorphism $\tau : R/(g) \to R/(f,g)$ is surjective with kernel (f), so

$$(R/(g))/(f) \cong R/(f,g).$$

A Truly Abstract Application

Thus we have the following result:

Theorem

Let f and g be elements in a commutative ring R. Then

$$R/(f,g) \cong [R/(f)]/(g) \cong [R/(g)]/(f),$$

More Specific Interesting Application

Applying this cute result to the ring $\mathbb{Z}[x]$ and the two principal ideals generated by $x^2 + 1$ and p, we have a truly marvelous result.

On the one hand, we have

$$\mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1) \cong \mathbb{Z}_p[x]/(x^2 + 1).$$

Then again, on the other hand, we have

$$\mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x])/(x^2 + 1)/(p) \cong \mathbb{Z}[i]/(p).$$

More Specific Interesting Application

Applying this cute result to the ring $\mathbb{Z}[x]$ and the two principal ideals generated by $x^2 + 1$ and p, we have a truly marvelous result.

On the one hand, we have

$$\mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1) \cong \mathbb{Z}_p[x]/(x^2 + 1).$$

Then again, on the other hand, we have

$$\mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x])/(x^2 + 1)/(p) \cong \mathbb{Z}[i]/(p).$$

More Specific Interesting Application

So, we have that

$$\mathbb{Z}_p[x]/(x^2+1) \cong \mathbb{Z}[i]/(p).$$

If R is a commutative ring and f is an element of R, then $R/(f)$ is an integral domain if and only if f is irreducible.

More Specific Interesting Application

Since

$$\mathbb{Z}_p[x]/(x^2+1) \cong \mathbb{Z}[i]/(p),$$

we see that x^2+1 is irreducible in $\mathbb{Z}_p[x]$ if and only if p is irreducible in $\mathbb{Z}[i]$.

More Specific Interesting Application

In $\mathbb{Z}_p[x]$, x^2+1 is reducible if and only if x^2+1 has a root in $\mathbb{Z}_p$.

In $\mathbb{Z}[i]$, p is reducible if and only if there are integers a and b so that $p=(a-bi)(a+bi)$. That is, if and only if $p=a^2+b^2$.

More Specific Interesting Application

In $\mathbb{Z}_p[x]$, x^2+1 is reducible if and only if x^2+1 has a root in $\mathbb{Z}_p$.

In $\mathbb{Z}[i]$, p is reducible if and only if there are integers a and b so that $p=(a-bi)(a+bi)$. That is, if and only if $p=a^2+b^2$.

More Specific Interesting Application

Putting this all together, we have that $x^2 + 1$ has a root in $\mathbb{Z}_p$, that is $x^2 + 1 = 0$ has an integral root $\mod p$, if and only if there exist integers a and b so that $p = (a - bi)(a + bi) = a^2 + b^2$.

This shows that (1) $\Leftrightarrow$ (3).

Thus, we've proved our conjecture:

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that $p = a^2 + b^2$.*
2. *p is congruent to 1 modulo 4*
3. *The polynomial $x^2 + 1$ has a root in the integers modulo p.*

We've proved it by applying the interesting isomorphism

$$R/(f,g) \cong [R/(f)]/(g) \cong [R/(g)]/(f),$$

Thus, we've proved our conjecture:

Theorem

Let p be an odd prime number. The following conditions are equivalent:

1. *There exist natural numbers a and b so that $p = a^2 + b^2$.*
2. *p is congruent to 1 modulo 4*
3. *The polynomial $x^2 + 1$ has a root in the integers modulo p.*

We've proved it by applying the interesting isomorphism

$$R/(f,g) \cong [R/(f)]/(g) \cong [R/(g)]/(f),$$

Thank you for attending!