Sums of two squares
A tale of two sums

Melanie Abel

Department of Mathematics
University of Maryland, College Park

Directed Reading Program, Fall 2016
Let $p$ be an odd prime number.

**Theorem (Fermat)**

$p$ is a sum of two squares iff $p \equiv 1 \pmod{4}$. 
Let \( p \) be an odd prime number.

**Theorem (Fermat)**

\( p \) is a sum of two squares iff \( p \equiv 1 \pmod{4} \).

**Proof (The first half).**

Let \( p \equiv 3 \pmod{4} \) and assume \( p = k_1^2 + k_2^2 \).
Let \( p \) be an odd prime number.

**Theorem (Fermat)**

\( p \) is a sum of two squares iff \( p \equiv 1 \quad (4) \).

**Proof (The first half).**

Let \( p \equiv 3 \quad (4) \) and assume \( p = k_1^2 + k_2^2 \).

Then \( k_1 \) and \( k_2 \) equal either 0 (4), 1 (4), 2 (4) or 3 (4).
Let $p$ be an odd prime number.

**Theorem (Fermat)**

$p$ is a sum of two squares iff $p \equiv 1 \ (4)$.

**Proof (The first half).**

Let $p \equiv 3 \ (4)$ and assume $p = k_1^2 + k_2^2$.
Then $k_1$ and $k_2$ equal either 0 (4), 1 (4), 2 (4) or 3 (4).
Thus $k_1^2$ and $k_2^2$ equal either 0 (4) or 1 (4).
Let $p$ be an odd prime number.

**Theorem (Fermat)**

$p$ is a sum of two squares iff $p \equiv 1 \pmod{4}$.

**Proof (The first half).**

Let $p \equiv 3 \pmod{4}$ and assume $p = k_1^2 + k_2^2$.

Then $k_1$ and $k_2$ equal either 0 (4), 1 (4), 2 (4) or 3 (4).

Thus $k_1^2$ and $k_2^2$ equal either 0 (4) or 1 (4).

Therefore $k_1^2 + k_2^2$ can only equal 0 (4), 1 (4) or 2 (4).
Wilson’s Theorem

If \( p \) is prime, then \((p - 1)! \equiv -1 \pmod{p}\).
Wilson’s Theorem and Corollary

Wilson’s Theorem

If \( p \) is prime, then \((p - 1)! \equiv -1 \pmod{p}\).

Corollary

If \( p \equiv 1 \pmod{4} \), we can solve \( x^2 \equiv -1 \pmod{p} \).
Wilson's Theorem and Corollary

Wilson's Theorem
If $p$ is prime, then $(p - 1)! \equiv -1 \ p$.

Corollary
If $p \equiv 1 \ 4$, we can solve $x^2 \equiv -1 \ p$.

Example
Wilson’s Theorem and Corollary

**Wilson's Theorem**

If $p$ is prime, then $(p - 1)! \equiv -1 \ (p)$.

**Corollary**

If $p \equiv 1 \ (4)$, we can solve $x^2 \equiv -1 \ (p)$.

**Example**

Let $p = 13$. Then, by Wilson’s Theorem, $12! \equiv -1 \ (13)$. 

$12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. 
## Wilson’s Theorem and Corollary

### Wilson’s Theorem

If $p$ is prime, then $(p - 1)! \equiv -1 \pmod{p}$.

### Corollary

If $p \equiv 1 \pmod{4}$, we can solve $x^2 \equiv -1 \pmod{p}$.

### Example

Let $p = 13$. Then, by Wilson’s Theorem, $12! \equiv -1 \pmod{13}$.

$12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

Taking remainder mod 13,

$12! \equiv (-1)(-2)(-3)(-4)(-5)(-6)(6)(5)(4)(3)(2)(1) \pmod{13}$. 
Wilson’s Theorem and Corollary

Wilson’s Theorem

If \( p \) is prime, then \((p - 1)! \equiv -1 \mod p\).

Corollary

If \( p \equiv 1 \mod 4\), we can solve \( x^2 \equiv -1 \mod p\).

Example

Let \( p = 13\). Then, by Wilson’s Theorem, \( 12! \equiv -1 \mod 13 \).

\[ 12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1. \]

Taking remainder mod 13,

\[ 12! \equiv (-1)(-2)(-3)(-4)(-5)(-6)(6)(5)(4)(3)(2)(1) \mod 13. \]

Pulling out \(-1\)s, we have \((-1)^6 \cdot (6!)^2 \equiv (6!)^2 \equiv -1 \mod 13\).
The Gaussian integers

Definition

The Gaussian integers are the set of complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$.

These act like integers in the following sense:
The Gaussian integers

**Definition**

The **Gaussian integers** are the set of complex numbers of the form \( a + bi \) where \( a, b \in \mathbb{Z} \).

These act like **integers** in the following sense:

Some **numbers** are **prime**, and every **number** factors uniquely into a product of **primes**.
Implications of the Norm

**Theorem**

A prime $p$ is either **prime** or can be factored into $(a + bi)(a - bi)$. 

Example

If $p \equiv 3 \pmod{4}$, $p$ is prime.
Implications of the Norm

**Theorem**

A prime $p$ is either prime or can be factored into $(a + bi)(a - bi)$.

**Corollary**

A prime $p$ is not prime iff $p = a^2 + b^2$. 
Implications of the Norm

**Theorem**

A prime \( p \) is either prime or can be factored into \((a + bi)(a - bi)\).

**Corollary**

A prime \( p \) is not prime iff \( p = a^2 + b^2 \).

**Example**

\[ 5 = 2^2 + 1^2 = (2 - i)(2 + i). \]
The case of 3 (4)

Wilson’s Theorem

The Gaussian Integers

Implications of the Norm

Factorization using Wilson’s Theorem

**Theorem**

A prime $p$ is either prime or can be factored into $(a + bi)(a - bi)$.

**Corollary**

A prime $p$ is not prime iff $p = a^2 + b^2$.

**Example**

$5 = 2^2 + 1^2 = (2 - i)(2 + i)$.

**Example**

If $p \equiv 3 \pmod{4}$, $p$ is prime.
Factorization using Wilson’s Theorem

**Theorem**

If \( p \equiv 1 \pmod{4} \), then \( p \) is not prime.
Factorization using Wilson’s Theorem

Theorem

If \( p \equiv 1 \pmod{4} \), then \( p \) is not prime.

Example

Consider \( p = 3301 \). By Wilson’s Theorem,
\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.
\]
Factorization using Wilson’s Theorem

Theorem

If \( p \equiv 1 \pmod{4} \), then \( p \) is not prime.

Example

Consider \( p = 3301 \). By Wilson’s Theorem,
\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.
\]
So \( 3301 \mid (1212 + i)(1212 - i) \).
Factorization using Wilson’s Theorem

Theorem

If \( p \equiv 1 \pmod{4} \), then \( p \) is not prime.

Example

Consider \( p = 3301 \). By Wilson’s Theorem,

\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.
\]

So \( 3301 | (1212 + i)(1212 - i) \).

But 3301 doesn’t divide \( 1212 + i \) or \( 1212 - i \).
Factorization using Wilson’s Theorem

**Theorem**

*If* \( p \equiv 1 \pmod{4} \), *then* \( p \) *is not prime.*

**Example**

Consider \( p = 3301 \). By Wilson’s Theorem,
\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.
\]
So \( 3301 \mid (1212 + i)(1212 - i) \).
But 3301 doesn’t divide \( 1212 + i \) or \( 1212 - i \).
So, 3301 is not *prime!*
Theorem

If $p \equiv 1 \pmod{4}$, then $p$ is not prime.

Example

Consider $p = 3301$. By Wilson’s Theorem, $(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}$. So $3301 | (1212 + i)(1212 - i)$.

But 3301 doesn’t divide $1212 + i$ or $1212 - i$.

So, 3301 is not prime!

$3301 \cdot 5 \cdot 49 = (1212 + i)(1212 - i)$. 
Theorem

If \( p \equiv 1 \ (4) \), then \( p \) is not prime.

Example

Consider \( p = 3301 \). By Wilson’s Theorem,
\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \ (3301).
\]
So
\[
3301 | (1212 + i)(1212 - i).
\]
But 3301 doesn’t divide 1212 + \( i \) or 1212 − \( i \).
So, 3301 is not prime!
3301 · 5 · 49 = (1212 + \( i \))(1212 − \( i \)).
3301(2 − \( i \))(2 + \( i \))(8 − 5\( i \))(8 + 5\( i \)) = (1212 + \( i \))(1212 − \( i \)).
Factorization using Wilson’s Theorem

**Theorem**

If \( p \equiv 1 \pmod{4} \), then \( p \) is not prime.

**Example**

Consider \( p = 3301 \). By Wilson’s Theorem,

\[
(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.
\]

So \( 3301 \mid (1212 + i)(1212 - i) \).

But 3301 doesn’t divide 1212 + \( i \) or 1212 − \( i \).

So, 3301 is not prime!

\[
3301 \cdot 5 \cdot 49 = (1212 + i)(1212 - i).
\]

\[
3301(2 - i)(2 + i)(8 - 5i)(8 + 5i) = (1212 + i)(1212 - i).
\]

\[
(1212 + i)/(2 + i) = (485 - 242i)
\]
The case of 3 (4)
Wilson's Theorem
The Gaussian Integers
Implications of the Norm
Factorization using Wilson's Theorem

Factorization using Wilson’s Theorem

**Theorem**

If $p \equiv 1 \ (4)$, then $p$ is not prime.

**Example**

Consider $p = 3301$. By Wilson’s Theorem,

$$(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \ (3301).$$

So $3301|(1212 + i)(1212 - i)$.

But 3301 doesn’t divide $1212 + i$ or $1212 - i$.

So, 3301 is not prime!

$3301 \cdot 5 \cdot 49 = (1212 + i)(1212 - i)$.

$3301(2 - i)(2 + i)(8 - 5i)(8 + 5i) = (1212 + i)(1212 - i)$.

$(1212 + i)/(2 + i) = (485 - 242i)/(8 + 5i) = 30 + 49i$. 
Factorization using Wilson’s Theorem

**Theorem**

*If* \( p \equiv 1 \pmod{4} \), *then* \( p \) *is not prime.*

**Example**

Consider \( p = 3301 \). By Wilson’s Theorem,
\[(1650!)^2 + 1 \equiv (1212)^2 + 1 \equiv 0 \pmod{3301}.\]

So \( 3301 | (1212 + i)(1212 - i) \).

But 3301 doesn’t divide 1212 + \( i \) or 1212 − \( i \).

So, 3301 is not prime!

\[
3301 \cdot 5 \cdot 49 = (1212 + i)(1212 - i).
\]

\[
3301(2 - i)(2 + i)(8 - 5i)(8 + 5i) = (1212 + i)(1212 - i).
\]

\[
(1212 + i)/(2 + i) = (485 - 242i)/(8 + 5i) = 30 + 49i.
\]

Thus \( 3301 = 30^2 + 49^2. \)