When is a prime not a prime?

Daniel Fretwell

School of Mathematics and Statistics, University of Sheffield

Semester 2, 2010/2011

...when it's ajar.

This talk is all about the quest for unique factorisation and why it should be important.

We have all known for a long time that any positive integer greater than 1 has a unique factorisation into prime numbers upto ordering (for example $21 = 3 \times 7 = 7 \times 3$ and $50 = 2 \times 5^2 = 5 \times 2 \times 5$).

...when it's ajar.

This talk is all about the quest for unique factorisation and why it should be important.

We have all known for a long time that any positive integer greater than 1 has a unique factorisation into prime numbers upto ordering (for example $21 = 3 \times 7 = 7 \times 3$ and $50 = 2 \times 5^2 = 5 \times 2 \times 5$).

How does this work if we allow negatives? Well here we have to allow for sign changes also but the actual primes that appear are still the same (e.g. $21 = 3 \times 7 = (-3) \times (-7)$). So really we can still consider the factorisation to be unique upto sign and ordering.

The important things here are the fact that we are working in the ring $\mathbb{Z}$ and that the "sign changing" elements ± 1 are the units of this ring. The prime numbers are the irreducibles of this ring.

How does this work if we allow negatives? Well here we have to allow for sign changes also but the actual primes that appear are still the same (e.g. $21 = 3 \times 7 = (-3) \times (-7)$). So really we can still consider the factorisation to be unique upto sign and ordering.

The important things here are the fact that we are working in the ring $\mathbb{Z}$ and that the "sign changing" elements ± 1 are the units of this ring. The prime numbers are the irreducibles of this ring.

What happens in other rings? Well in order to answer this question we have to think about what kind of rings we want to consider as “other rings”.

We will construct rings that behave most like the integers and study factorisation in these rings. It will turn out that we do not always have unique factorisation into irreducibles but that we can actually restore unique factorisation if we look not at the elements but at the ideals.

Along the way we will see how unique factorisation can help when solving Diophantine equations. Also we will see a nice theorem that helps us to get a prime ideal factorisation of ideals generated by prime numbers, showing us that often prime numbers factorise further in bigger rings (hence the title of the project).

What happens in other rings? Well in order to answer this question we have to think about what kind of rings we want to consider as “other rings”.

We will construct rings that behave most like the integers and study factorisation in these rings. It will turn out that we do not always have unique factorisation into irreducibles but that we can actually restore unique factorisation if we look not at the elements but at the ideals.

Along the way we will see how unique factorisation can help when solving Diophantine equations. Also we will see a nice theorem that helps us to get a prime ideal factorisation of ideals generated by prime numbers, showing us that often prime numbers factorise further in bigger rings (hence the title of the project).

What happens in other rings? Well in order to answer this question we have to think about what kind of rings we want to consider as “other rings”.

We will construct rings that behave most like the integers and study factorisation in these rings. It will turn out that we do not always have unique factorisation into irreducibles but that we can actually restore unique factorisation if we look not at the elements but at the ideals.

Along the way we will see how unique factorisation can help when solving Diophantine equations. Also we will see a nice theorem that helps us to get a prime ideal factorisation of ideals generated by prime numbers, showing us that often prime numbers factorise further in bigger rings (hence the title of the project).

Outline of talk

Generalizing the integers

We make a definition:

Definition

A number field is a field $K \supseteq \mathbb{Q}$ such that the degree of the field extension $K/\mathbb{Q}$ is finite. We refer to the degree of a number field as the degree of the field extension $K/\mathbb{Q}$, i.e. the dimension of K as a $\mathbb{Q}$-vector space.

Examples

The fields:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and

$$\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 \mid a, b, c \in \mathbb{Q}\}$$

are number fields. They have degrees 2 and 3 respectively.

Generalizing the integers

We make a definition:

Definition

A number field is a field $K \supseteq \mathbb{Q}$ such that the degree of the field extension $K/\mathbb{Q}$ is finite. We refer to the degree of a number field as the degree of the field extension $K/\mathbb{Q}$, i.e. the dimension of K as a $\mathbb{Q}$-vector space.

Examples

The fields:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and

$$\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 \mid a, b, c \in \mathbb{Q}\}$$

are number fields. They have degrees 2 and 3 respectively.

Actually, every number field contains a special ring inside it, the ring of integers.

Definition

The ring of integers of a number field K is the set:

$$\mathfrak{O}_K = \{\alpha \in K \mid \alpha \text{ satisfies a monic polynomial over } \mathbb{Z}\}.$$

Examples

When $K = \mathbb{Q}$ we have that $\mathfrak{O}_K = \mathbb{Z}$. When $K = \mathbb{Q}(i)$ we have that $\mathfrak{O}_K = \mathbb{Z}[i]$. When $K = \mathbb{Q}(\zeta_n)$ for any primitive nth root of unity ζ_n we have that $\mathfrak{O}_K = \mathbb{Z}[\zeta_n]$.

Actually, every number field contains a special ring inside it, the ring of integers.

Definition

The ring of integers of a number field K is the set:

$$\mathfrak{O}_K = \{\alpha \in K \mid \alpha \text{ satisfies a monic polynomial over } \mathbb{Z}\}.$$

Examples

When $K = \mathbb{Q}$ we have that $\mathfrak{O}_K = \mathbb{Z}$. When $K = \mathbb{Q}(i)$ we have that $\mathfrak{O}_K = \mathbb{Z}[i]$. When $K = \mathbb{Q}(\zeta_n)$ for any primitive nth root of unity ζ_n we have that $\mathfrak{O}_K = \mathbb{Z}[\zeta_n]$.

However, the ring of integers of a number field $K = \mathbb{Q}(\theta)$ is not always $\mathbb{Z}[\theta]$.

When we take $K = \mathbb{Q}(\sqrt{5})$ we have that $\frac{1+\sqrt{5}}{2} \in \mathfrak{O}_K$ so that the ring of integers is "bigger" than $\mathbb{Z}[\sqrt{5}]$.

There are general ways to work out what ring $\mathfrak{O}_K$ is, but we do not have time to go into this here. For quadratic number fields $K = \mathbb{Q}(\sqrt{d})$, it turns out that the value we get when reducing d mod 4 completely determines what the ring of integers will be (d is of course square-free here).

The ring of integers should be thought of as a generalisation of the notion of integer. It mimics the inclusion of $\mathbb{Z}$ inside $\mathbb{Q}$. Also, studying $\mathfrak{O}_K$ helps us to understand the number field K.

However, the ring of integers of a number field $K = \mathbb{Q}(\theta)$ is not always $\mathbb{Z}[\theta]$.

When we take $K = \mathbb{Q}(\sqrt{5})$ we have that $\frac{1+\sqrt{5}}{2} \in \mathfrak{O}_K$ so that the ring of integers is "bigger" than $\mathbb{Z}[\sqrt{5}]$.

There are general ways to work out what ring $\mathfrak{O}_K$ is, but we do not have time to go into this here. For quadratic number fields $K = \mathbb{Q}(\sqrt{d})$, it turns out that the value we get when reducing d mod 4 completely determines what the ring of integers will be (d is of course square-free here).

The ring of integers should be thought of as a generalisation of the notion of integer. It mimics the inclusion of $\mathbb{Z}$ inside $\mathbb{Q}$. Also, studying $\mathfrak{O}_K$ helps us to understand the number field K.

However, the ring of integers of a number field $K = \mathbb{Q}(\theta)$ is not always $\mathbb{Z}[\theta]$.

When we take $K = \mathbb{Q}(\sqrt{5})$ we have that $\frac{1+\sqrt{5}}{2} \in \mathfrak{O}_K$ so that the ring of integers is "bigger" than $\mathbb{Z}[\sqrt{5}]$.

There are general ways to work out what ring $\mathfrak{O}_K$ is, but we do not have time to go into this here. For quadratic number fields $K = \mathbb{Q}(\sqrt{d})$, it turns out that the value we get when reducing d mod 4 completely determines what the ring of integers will be (d is of course square-free here).

The ring of integers should be thought of as a generalisation of the notion of integer. It mimics the inclusion of $\mathbb{Z}$ inside $\mathbb{Q}$. Also, studying $\mathfrak{O}_K$ helps us to understand the number field K.

It turns out that in $\mathfrak{O}_K$, factorisation into irreducibles is always possible (this is a consequence of $\mathfrak{O}_K$ being Noetherian).

However, is it always unique? By unique we mean the same as in the integer case, unique upto ordering and multiplication by units.

Unfortunately the answer is no.

Example

Take the number field $K = \mathbb{Q}(\sqrt{-5})$. Here we have that $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the units are ± 1. In this ring we have two completely different factorisations of 6 into irreducibles:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$

It turns out that in $\mathfrak{O}_K$, factorisation into irreducibles is always possible (this is a consequence of $\mathfrak{O}_K$ being Noetherian).

However, is it always unique? By unique we mean the same as in the integer case, unique upto ordering and multiplication by units.

Unfortunately the answer is no.

Example

Take the number field $K = \mathbb{Q}(\sqrt{-5})$. Here we have that $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the units are ± 1. In this ring we have two completely different factorisations of 6 into irreducibles:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$

It turns out that in $\mathfrak{O}_K$, factorisation into irreducibles is always possible (this is a consequence of $\mathfrak{O}_K$ being Noetherian).

However, is it always unique? By unique we mean the same as in the integer case, unique upto ordering and multiplication by units.

Unfortunately the answer is no.

Example

Take the number field $K = \mathbb{Q}(\sqrt{-5})$. Here we have that $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the units are ± 1. In this ring we have two completely different factorisations of 6 into irreducibles:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$

Outline of talk

Solving $x^2 + 2 = y^3$

If the ring of integers does happen to have unique factorisation into irreducibles then we can often use this fact to solve Diophantine equations.

Fermat once conjectured that the equation $x^2 + 2 = y^3$ has only two solutions in integers, namely $(x, y) = (\pm 5, 3)$. This is a hard problem to solve using elementary methods.

However, if we work in the number field $K = \mathbb{Q}(\sqrt{-2})$, which has ring of integers $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$, we may factorise and get:

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$$

It is easily shown that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain (using the norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$) and so it is a unique factorisation domain.

Solving $x^2 + 2 = y^3$

If the ring of integers does happen to have unique factorisation into irreducibles then we can often use this fact to solve Diophantine equations.

Fermat once conjectured that the equation $x^2 + 2 = y^3$ has only two solutions in integers, namely $(x, y) = (\pm 5, 3)$. This is a hard problem to solve using elementary methods.

However, if we work in the number field $K = \mathbb{Q}(\sqrt{-2})$, which has ring of integers $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$, we may factorise and get:

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$$

It is easily shown that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain (using the norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$) and so it is a unique factorisation domain.

Solving $x^2 + 2 = y^3$

If the ring of integers does happen to have unique factorisation into irreducibles then we can often use this fact to solve Diophantine equations.

Fermat once conjectured that the equation $x^2 + 2 = y^3$ has only two solutions in integers, namely $(x, y) = (\pm 5, 3)$. This is a hard problem to solve using elementary methods.

However, if we work in the number field $K = \mathbb{Q}(\sqrt{-2})$, which has ring of integers $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$, we may factorise and get:

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$$

It is easily shown that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain (using the norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$) and so it is a unique factorisation domain.

Solving $x^2 + 2 = y^3$

Now we have to have that both x and y are odd (simple check mod 4) but in this case the two elements $(x + \sqrt{-2})$ and $(x - \sqrt{-2})$ of $\mathbb{Z}[\sqrt{-2}]$ can be shown to be coprime.

The right hand side of our Diophantine equation is a cube number. Thus uniqueness of factorisation in $\mathbb{Z}[\sqrt{-2}]$ now tells us that $(x + \sqrt{-2}) = u(a + b\sqrt{-2})^3$ for some unit u of $\mathbb{Z}[\sqrt{-2}]$ and some pair of integers a, b. The only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1 so we may assume that $u = 1$ (since both units are cubes themselves).

Expanding the above and equating coefficients tells us that $1 = b(3a^2 - 2b^2)$, immediately giving that $b = \pm 1$ and $a = 1$. Substituting these solutions for a and b in the above gives to us the only two possible solutions of our problem, $(x, y) = (\pm 5, 3)$.

Outline of talk

Looking elsewhere

How can we achieve unique factorisation from a setting that does not have it?

The natural thought would be to add more elements so that the counter-examples all factorise further into things that really are the same factorisation.

Fortunately we do not have to do this. In the late 19th Century, Dedekind was able to use the work of Kummer to achieve unique factorisation without adding extra elements. However he realised the need to work with ideals rather than elements.

Looking elsewhere

How can we achieve unique factorisation from a setting that does not have it?

The natural thought would be to add more elements so that the counter-examples all factorise further into things that really are the same factorisation.

Fortunately we do not have to do this. In the late 19th Century, Dedekind was able to use the work of Kummer to achieve unique factorisation without adding extra elements. However he realised the need to work with ideals rather than elements.

Looking elsewhere

How can we achieve unique factorisation from a setting that does not have it?

The natural thought would be to add more elements so that the counter-examples all factorise further into things that really are the same factorisation.

Fortunately we do not have to do this. In the late 19th Century, Dedekind was able to use the work of Kummer to achieve unique factorisation without adding extra elements. However he realised the need to work with ideals rather than elements.

The big breakthrough

Dedekind proved the following:

Theorem

Every non-zero proper ideal of $\mathcal{O}_K$ can be factorised uniquely into prime ideals. The factorisation is unique upto ordering of the prime ideals.

Recall that a proper ideal $\mathfrak{p}$ of a ring R is prime if it has the property that whenever $a, b \in R$ are such that $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

The above is a major achievement. We do not even have to worry about units now.

The big breakthrough

Dedekind proved the following:

Theorem

Every non-zero proper ideal of $\mathfrak{O}_K$ can be factorised uniquely into prime ideals. The factorisation is unique upto ordering of the prime ideals.

Recall that a proper ideal $\mathfrak{p}$ of a ring R is prime if it has the property that whenever $a, b \in R$ are such that $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

The above is a major achievement. We do not even have to worry about units now.

The big breakthrough

Dedekind proved the following:

Theorem

Every non-zero proper ideal of $\mathfrak{O}_K$ can be factorised uniquely into prime ideals. The factorisation is unique upto ordering of the prime ideals.

Recall that a proper ideal $\mathfrak{p}$ of a ring R is prime if it has the property that whenever $a, b \in R$ are such that $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

The above is a major achievement. We do not even have to worry about units now.

Recall earlier that we had the following example of non-uniqueness of factorisation into irreducibles in $\mathbb{Z}[\sqrt{-5}]$:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2.3$$

In terms of prime ideal factorisation this is explained by a reordering of prime ideals in the factorisation of the ideal generated by 6:

$$\langle 6 \rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_1\mathfrak{p}_3 = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$$

where $\mathfrak{p}_1 = \langle 2, \sqrt{-5} + 1 \rangle, \mathfrak{p}_2 = \langle 3, \sqrt{-5} + 1 \rangle, \mathfrak{p}_3 = \langle 3, \sqrt{-5} - 1 \rangle$.

Recall earlier that we had the following example of non-uniqueness of factorisation into irreducibles in $\mathbb{Z}[\sqrt{-5}]$:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2.3$$

In terms of prime ideal factorisation this is explained by a reordering of prime ideals in the factorisation of the ideal generated by 6:

$$\langle 6 \rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_1\mathfrak{p}_3 = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$$

where $\mathfrak{p}_1 = \langle 2, \sqrt{-5} + 1 \rangle, \mathfrak{p}_2 = \langle 3, \sqrt{-5} + 1 \rangle, \mathfrak{p}_3 = \langle 3, \sqrt{-5} - 1 \rangle$.

Ok, so we know that in $\mathfrak{O}_K$ the non-zero proper ideals factorise uniquely into prime ideals upto order but how do we actually find the factorisation?

Dedekind found out how for ideals generated by primes $p \in \mathbb{Z}$:

Theorem

Let $K = \mathbb{Q}(\theta)$ be a number field generated by some algebraic integer θ. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Z}$.
If $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$ then the factorisation into distinct monic irreducibles mod p:

$$f(x) \equiv f_1(x)^{e_1} \dots f_g(x)^{e_g} \bmod p$$

gives the unique prime ideal factorisation:

$$\langle p \rangle = \prod_{i=1}^{g} \langle p, f_i(\theta) \rangle^{e_i}.$$

Ok, so we know that in $\mathfrak{O}_K$ the non-zero proper ideals factorise uniquely into prime ideals upto order but how do we actually find the factorisation?

Dedekind found out how for ideals generated by primes $p \in \mathbb{Z}$:

Theorem

Let $K = \mathbb{Q}(\theta)$ be a number field generated by some algebraic integer θ. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Z}$.
If $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$ then the factorisation into distinct monic irreducibles mod p:

$$f(x) \equiv f_1(x)^{e_1} \dots f_g(x)^{e_g} \bmod p$$

gives the unique prime ideal factorisation:

$$\langle p \rangle = \prod_{i=1}^{g} \langle p, f_i(\theta) \rangle^{e_i}.$$

Ok, so we know that in $\mathfrak{O}_K$ the non-zero proper ideals factorise uniquely into prime ideals upto order but how do we actually find the factorisation?

Dedekind found out how for ideals generated by primes $p \in \mathbb{Z}$:

Theorem

Let $K = \mathbb{Q}(\theta)$ be a number field generated by some algebraic integer θ. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Z}$.
If $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$ then the factorisation into distinct monic irreducibles mod p:

$$f(x) \equiv f_1(x)^{e_1} \dots f_g(x)^{e_g} \bmod p$$

gives the unique prime ideal factorisation:

$$\langle p \rangle = \prod_{i=1}^{g} \langle p, f_i(\theta) \rangle^{e_i}.$$

This result suggests that some prime numbers actually factorise further in rings of integers that are "bigger" than $\mathbb{Z}$. We can see this in action here:

Example

Start with the number field $K = \mathbb{Q}(\sqrt{-5})$. This has ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Now $\sqrt{-5}$ has minimal polynomial $x^2 + 5$ over $\mathbb{Q}$.

Working mod 2 we get the factorisation
$x^2 + 5 \equiv (x+1)^2 \bmod 2$, so that $\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle^2$.

Working mod 3 we get the factorisation
$x^2 + 5 \equiv (x+1)(x-1) \bmod 3$, so that
$\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle$.

Notice that $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$, and the above agrees with the factorisation of $\langle 6 \rangle$ we had earlier!

This result suggests that some prime numbers actually factorise further in rings of integers that are "bigger" than $\mathbb{Z}$. We can see this in action here:

Example

Start with the number field $K = \mathbb{Q}(\sqrt{-5})$. This has ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Now $\sqrt{-5}$ has minimal polynomial $x^2 + 5$ over $\mathbb{Q}$.

Working mod 2 we get the factorisation $x^2 + 5 \equiv (x+1)^2 \bmod 2$, so that $\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle^2$.

Working mod 3 we get the factorisation $x^2 + 5 \equiv (x+1)(x-1) \bmod 3$, so that $\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle$.

Notice that $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$, and the above agrees with the factorisation of $\langle 6 \rangle$ we had earlier!

This result suggests that some prime numbers actually factorise further in rings of integers that are "bigger" than $\mathbb{Z}$. We can see this in action here:

Example

Start with the number field $K = \mathbb{Q}(\sqrt{-5})$. This has ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Now $\sqrt{-5}$ has minimal polynomial $x^2 + 5$ over $\mathbb{Q}$.

Working mod 2 we get the factorisation $x^2 + 5 \equiv (x + 1)^2 \bmod 2$, so that $\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle^2$.

Working mod 3 we get the factorisation $x^2 + 5 \equiv (x + 1)(x - 1) \bmod 3$, so that $\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle$.

Notice that $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$, and the above agrees with the factorisation of $\langle 6 \rangle$ we had earlier!

This result suggests that some prime numbers actually factorise further in rings of integers that are "bigger" than $\mathbb{Z}$. We can see this in action here:

Example

Start with the number field $K = \mathbb{Q}(\sqrt{-5})$. This has ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Now $\sqrt{-5}$ has minimal polynomial $x^2 + 5$ over $\mathbb{Q}$.

Working mod 2 we get the factorisation
$x^2 + 5 \equiv (x + 1)^2 \bmod 2$, so that $\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle^2$.

Working mod 3 we get the factorisation
$x^2 + 5 \equiv (x + 1)(x - 1) \bmod 3$, so that
$\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle$.

Notice that $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$, and the above agrees with the factorisation of $\langle 6 \rangle$ we had earlier!

This result suggests that some prime numbers actually factorise further in rings of integers that are "bigger" than $\mathbb{Z}$. We can see this in action here:

Example

Start with the number field $K = \mathbb{Q}(\sqrt{-5})$. This has ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Now $\sqrt{-5}$ has minimal polynomial $x^2 + 5$ over $\mathbb{Q}$.

Working mod 2 we get the factorisation
$x^2 + 5 \equiv (x + 1)^2 \bmod 2$, so that $\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle^2$.

Working mod 3 we get the factorisation
$x^2 + 5 \equiv (x + 1)(x - 1) \bmod 3$, so that
$\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle$.

Notice that $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$, and the above agrees with the factorisation of $\langle 6 \rangle$ we had earlier!

That's all folks

The end.