Sums of Two Squares

These are notes for my lecture of November 3. I will discuss the sums of two squares using slightly different methods from the book.

Gauss studied binary quadratic forms in his famous book *Disquisitiones Arithmeticae*. Many of the results are now standard material, but are usually talked about in the language of quadratic fields. By a *quadratic field* I mean a field like $\mathbb{Q}(i)$, the field of $a + bi$ with $a, b \in \mathbb{Q}$, or $\mathbb{Q}(\sqrt{5})$, the field of $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$. Ideals of rings in quadratic fields are closely related to binary quadratic forms.

I will assume you remember results and notations from two other posted notes:

http://sporadic.stanford.edu/bump/ideals.pdf


In *conic.pdf* we saw that if $F$ is a field and $D \in F$ is a nonsquare, then we can construct a field $K = F(\sqrt{D})$ which is a two dimensional vector space over $F$ in which $D$ has a square root $\sqrt{D}$. We also showed that there is a *norm map* $N: K \to F$ such that

$$N(x + y\sqrt{D}) = x^2 - Dy^2$$

(when $x, y \in F$) and $N(zw) = N(z)N(w)$.

**Remark 1.** If $F = \mathbb{Q}$ then $x^2 - Dy^2$ is a binary quadratic form, and we can study binary quadratic forms using this fact. This observation might seem to have a limitation: can we only study $ax^2 + bxy + cy^2$ this way when $b = 0$? Luckily, no, as the following example shows. Let $K = \mathbb{Q}(\sqrt{-3})$. Let $\rho = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. Thus $\rho \in K$. Let us compute the norm of $x + y\rho$. We have

$$N(x + y\rho) = (x + y\rho)(x + y\rho)$$

where the bar is complex conjugation. (Avoid changing coordinates by writing everything in terms of $\sqrt{-3}$ – this way is easier.) Now the complex conjugate $\bar{\rho} = -\frac{1}{2} - \frac{\sqrt{-3}}{2} = \rho^2$ so

$$N(x + y\rho) = (x + y\rho)(x + y\rho) = x^2 + (\rho + \rho^2)xy + y^2\rho^3.$$  

We have $\rho + \rho^2 = -1$ and $\rho^3 = 1$ so $N(x + y\rho) = x^2 - xy + y^2$. So this technique can be used to study this quadratic form.

The goal in these notes is to determine which integers are representable as sums of two squares.

**Proposition 2.** If $m, n \in \mathbb{Z}$ are representable as sums of two squares then so is $mn$.

**Proof.** This follows from the identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x_3^2 + y_3^2$$  

(1)

where $x_3 = x_1x_2 - y_1y_2$ and $y_3 = x_1y_2 + x_2y_1$, since if $m = x_1^2 + y_1^2$ and $n = x_2^2 + y_2^2$ are sums of two squares then so is $mn = x_3^2 + y_3^2$. □
The identity (1) is just the identity $N(zw) = N(z)N(w)$ with $z = x_1 + iy_1$ and $w = x_2 + iy_2$. As you can imagine, this same trick can be used to study other binary quadratic forms. It can also be used to study quaternary quadratic forms, for example the sums of four squares:

**Proposition 3.** If $m, n$ are representable as sums of four squares then so is $mn$.

**Proof.** This depends on the identity 

$$(x_1^2+y_1^2+z_1^2+w_1^2)(x_2^2+y_2^2+z_2^2+w_2^2) = x_3^2+y_3^2+z_3^2+w_3^2,$$

where

$$
\begin{align*}
x_3 &= x_1x_2 - y_1y_2 - z_1z_2 - w_1w_2, \\
y_3 &= x_1y_2 + y_1x_2 + z_1w_2 - w_1z_2, \\
z_3 &= x_1z_2 - y_1w_2 + z_1x_2 + w_1y_2, \\
w_3 &= x_1w_2 + y_1z_2 - z_1y_2 + w_1x_2.
\end{align*}
$$

This also has an explanation in terms of a “norm map”, from the quaternion ring, a non-commutative ring that is a four dimensional algebra. But this trick doesn’t work to study quadratic forms in three variables, or five. It is quite special.

Now we need some facts about the ring $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ of Gaussian integers. Please review ideals and principal ideals from ideals.pdf. Remember this notation:

**Example.** If $R$ is any ring and $a \in R$ then $aR = (a)$ is defined to be the set of all multiples of $R$. That is,

$$(a) = \{na | n \in R\}.$$

This is an ideal, and an ideal of this form is called principal.

**Lemma. (Division Algorithm for Gaussian Integers)** Let $a, b \in \mathbb{Z}[i]$ and suppose that $b \neq 0$. Then there exist $q$ and $r \in \mathbb{Z}[i]$ such that $a = qb + r$ and $|r| < |b|$.

**Proof.** Let $\Lambda = (b)$ be the principal ideal generated by $b$. Since the vertices of $\mathbb{Z}[i]$ form a square lattices, $\Lambda$ is a square lattice, that is, the complex plane is tiled by squares, a typical one having vertices

$$xb, \quad (x+1)b, \quad (x+i)b, \quad (x+1+i)b. \tag{2}$$

We may put $a$ in one of these squares. The closest element of $\Lambda$ to $a$ is then one of (2), say $qb$ where $q = x, x + 1, x + i$ or $x + 1 + i$. Because these are the vertices of a square with side $|b|$, we have $|a - bq| \leq \frac{1}{\sqrt{2}}|b|$, so $|r| \leq \frac{1}{\sqrt{2}}|b| < |b|$.

**Proposition 4.** The ring $\mathbb{Z}[i]$ is a principal ideal domain: this means that every ideal is a principal ideal.
Proof. Let $I$ be an ideal of $\mathbb{Z}[i]$. If $I = \{0\}$ then we may take $b = 0$ and $I = (b)$. We may therefore assume that $I \neq \{0\}$. Let $b$ be a nonzero element of $I$ that minimizes $|b|$. Then we will show $I = (b)$. It follows from the fact that $b \in I$ and $I$ is an ideal that $(b) \subseteq I$, so we have to prove $I \subseteq (b)$. Let $a \in I$. Using the division algorithm for Gaussian integers write $a = bq + r$ with $|r| < |b|$. Then $r = 1 \cdot a - q \cdot b \in I$ since $I$ is an ideal and $a, b \in I$. Because $b$ is a nonzero element of $I$ of minimal length we have $r = 0$ so $a = bq \in (b)$ proving that $I \subseteq (b)$ and so $I = (b)$ is a principal ideal. \qed

We recall the following definitions. An element $\epsilon$ of a ring $R$ is called a unit if $\epsilon \delta = \delta \epsilon = 1$ for some $\delta \in R$. (The units in $\mathbb{Z}[i]$ are $1, -1, i$ and $-i$.) The units of any ring are denoted $R^*$ and form a group under multiplication. Restricting ourselves to commutative rings (preferably subrings of fields), elements $x$ and $y$ are called associates if $x = \epsilon y$ for some unit $\epsilon$. An element $\pi \in R$ is called irreducible if $\pi$ is nonzero, not a unit, and whenever we factor $\pi = xy$ either $x$ is a unit or $y$ is a unit. The term “irreducible” is more or less used interchangeably with the word prime if $R$ is a principal ideal domain, but for general rings, it is more correct to use the term prime to refer to ideals than elements. Anyway, even in a principal ideal domain such as $\mathbb{Z}[i]$ if we are thinking of primes we would not regard two irreducible elements as being different primes if they are associates. For example, $2 + i$ and $-1 + 2i$ are different elements of $\mathbb{Z}[i]$ but they are not different as primes since they are not associates.

Proposition 5. If $\pi$ is an irreducible (prime) element of $\mathbb{Z}[i]$ and $\alpha, \beta \in \mathbb{Z}[i]$ then $\pi | \alpha \beta$ implies $\pi | \alpha$ or $\pi | \beta$.

Proof. See ideals.pdf, the proof of the very last Proposition. \qed

Proposition 6. If $\pi$ is an irreducible element of $\mathbb{Z}[i]$ and $\pi | \alpha_1 \cdots \alpha_n$ then $\pi | \alpha_i$ for some $i$.

Proof. By the last proposition with $\alpha = \alpha_1$ and $\beta = \alpha_2 \cdots \alpha_n$, either $\pi | \alpha$ or $\pi | \beta$; in the second case, by induction on $n$, $\pi$ divides one of $\alpha_2, \ldots, \alpha_n$. \qed

Theorem 7. $\mathbb{Z}[i]$ is a unique factorization domain.

In other words if we have two factorizations

$$\alpha = \pi_1 \cdots \pi_n = \pi'_1 \cdots \pi'_m$$

of $\alpha \in \mathbb{Z}[i]$ into irreducible elements $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_m$, then $n = m$ and the $\pi'_i$ are associates of the $\pi_i$ in some order.

Proof. Since $\pi_1 | \alpha$, $\pi_1$ divides the product $\pi'_1 \cdots \pi'_m$. Thus it divides one of the $\pi'_i$, and reordering them, we may assume without loss of generality that $\pi_1 | \pi'_1$. Since both are prime, they are associates. If $\pi'_1 = \pi_1 \epsilon$ with $\epsilon$ a unit, we have $\pi_2 \cdots \pi_n = (\epsilon \pi'_2) \pi'_3 \cdots \pi'_m$, and by induction on $n$, $n - 1 = m - 1$ and $\epsilon \pi'_2, \ldots, \pi'_m$ are associates of $\pi_2, \ldots, \pi_n$ in some order. \qed

Theorem 8. (Fermat) Let $p$ be an odd prime (in $\mathbb{Z}$). Then $p$ is a sum of two squares if and only if $p \equiv 1 \mod 4$. 
Proof. If \( p \equiv 3 \mod 4 \) you showed on the midterm that \( p \) is not a sum of two squares. So we may assume that \( p \equiv 1 \mod 4 \). We have
\[
\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} = 1
\]
by Euler’s criterion since \( p \equiv 1 \mod 4 \), so \( \frac{p-1}{2} \) is even. Since \(-1\) is thus a quadratic residue we may find \( c \in \mathbb{Z} \) such that \( p|c^2 - 1 \) (in \( \mathbb{Z} \), hence also in \( \mathbb{Z}[i] \)). Let \( \pi \) be the greatest common divisor of \( p \) and \( c + i \) in \( \mathbb{Z}[i] \). We will show that \( \pi \) is prime and \( N(\pi) = p \). Note that this is enough since writing \( \pi = a + bi \) with \( a, b \in \mathbb{Z} \) this means that \( p = a^2 + b^2 \).

We will use the norm map. We have \( \pi|p \) and so \( N(\pi)|N(p) \) in \( \mathbb{Z} \). Note that \( N(p) = p^2 \), so \( N(\pi) = 1, p \) or \( p^2 \). We will show that \( N(\pi) \neq p^2 \) and \( N(\pi) \neq 1 \).

If \( N(\pi) = p^2 \) then since \( \pi|p \) we may write \( p = \pi \varepsilon \) for some \( \varepsilon \). We have \( p^2 = N(p) = N(\pi)N(\varepsilon) = p^2N(\varepsilon) \) so \( N(\varepsilon) = 1 \). This implies that \( \varepsilon \) is a unit and so \( p \) and \( \pi \) are associates. Now \( \pi|c + i \) but \( p \nmid c + i \) since \( \frac{c + i}{p} \) is not a Gaussian integer. (Its imaginary part is \( \frac{1}{p} \).) This is a contradiction.

If \( N(\pi) = 1 \) then \( \pi \) is a unit and so \( p, c + i \) are relatively prime. Taking complex conjugates, \( p \) and \( c - i \) are also relatively prime. Thus \( p \) and \( (c + i)(c - i) \) are relatively prime, but this is a contradiction since \( p|c^2 + 1 = (c + i)(c - i) \).

The only possibility that remains is \( N(\pi) = p \), so \( p = a^2 + b^2 \). \( \square \)