LECTURE 11 : GAUSSIAN INTEGERS APPLIED

- Begin by supplying some proof of certain assertions made in LECTURE 10. I provided plausibility by example last time, now we give explicit proof.

Thm (DIVISION ALGORITHM IN $\mathbb{Z}[i]$)

Let $z = a+bi$ and $w = c+di \in \mathbb{Z}[i]$.
Then $\exists\, q, r \in \mathbb{Z}[i]$ such that

$$z = qw + r$$

with $|r|^2 < |w|^2$ (a.k.a. norm(r) < norm(w))

Proof (following Shifrin's, "Abstract Algebra: A Geometric Approach" section 4.3, pg. 140 proof of Prop. 3.1 verbatim)

Consider the complex # $\frac{z}{w} = \frac{a+bi}{c+di} = x+yi \in \mathbb{Q}[i]$

and choose $m, n \in \mathbb{Z}$ such that

$$|m-x| \leq 1/2 \quad \text{and} \quad |n-y| \leq 1/2.$$

Set $q = m+ni$ and $r = z - qw$. Observe, for $w \neq 0$,

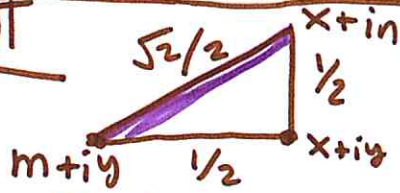
$$|r|^2 < |w|^2 \iff \left|\frac{r}{w}\right| < 1 \iff \left|\frac{z}{w} - q\right| < 1.$$

However, by construction of m, n and r,

$$\left|\frac{z}{w} - q\right| = |(x+yi) - (m+ni)| = \sqrt{(x-m)^2+(y-n)^2} \leq \frac{\sqrt{2}}{2}$$

(Oops, Δ-ineq not sharp enough here. See the triangle for why $\frac{\sqrt{2}}{2}$ reasonable.)

$\leq |x-m| + |i(y-n)|$ ~~$\leq \frac{1}{2}$~~



Hence, $\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{2}}{2} < 1 \iff |r|^2 < |w|^2$ and the Thm follows. //

Example (1) $z = -4+2i$ and $w = 3+2i$ (Shifrin p. 140)

$$\frac{z}{w} = \frac{-4+2i}{3+2i} = \frac{-8+14i}{13} \leftarrow \left[\text{multiplied by } \left(\frac{3-2i}{3-2i}\right)\right]$$

Set $q = -1+i$ (-1 close to $\frac{-8}{13}$ and i close to $\frac{14i}{13}$)

Hence $r = (-4+2i) - (-1+i)(3+2i)$

$= -4+2i - (-3-2i+3i-2)$

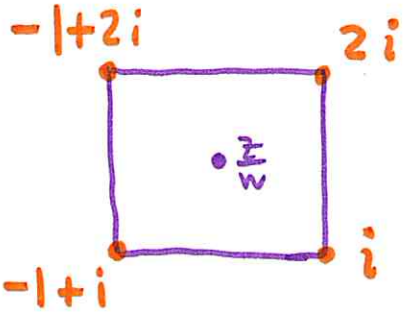
$= 1+i.$

Thus, $\underbrace{-4+2i}_{z} = \underbrace{(3+2i)}_{w}\underbrace{(-1+i)}_{q} + \underbrace{(1+i)}_{r}$

You can easily verify $\text{norm}(r) < \text{norm}(w)$.

Example (2) find $\gcd(\underbrace{1-5i}_{w}, \underbrace{7+4i}_{z})$

$$\frac{z}{w} = \frac{7+4i}{1-5i}\left[\frac{1+5i}{1+5i}\right] = \frac{-13+39i}{26} = \frac{-1+3i}{2}$$



all corners same distance from z/w
↪ q not unique.

Use $q = i$ for simplicity $\Rightarrow$ $\underbrace{z = i(1-5i) + 2 + 3i}_{\text{remainder}}$

thus

$(7+4i, 1-5i) = (z, w)$

$(1-5i, 2+3i) = (w, z - iw)$

Next we work out $\frac{1-5i}{2+3i}\left[\frac{2-3i}{2-3i}\right] = \frac{-13-13i}{13} = -1-i$

thus $(1-5i) = (-1-i)(2+3i)$.

Example ② continued

We found $1-5i = (-1-i)(2+3i)$ which shows $2+3i \mid 1-5i$ thus the Euclidean algorithm halts here

$$(7+4i, 1-5i) \longmapsto (1-5i, 2+3i) \quad \text{[HALT!]}$$

$$(z, w) \longmapsto (w, z - iw)$$

and, for essentially the same logic as in $\mathbb{Z}$, we conclude $\underline{\gcd(7+4i, 1-5i) = 2+3i}$ and

$$\underline{z - iw = (7+4i) - i(1-5i) = 2+3i}.$$

Proof of Euclidean Algorithm in $\mathbb{Z}[i]$: See Lecture 2 or §3 of the Mod. arithmetic.pdf. These arguments transfer to $\mathbb{Z}[i]$ as we have the needed division algorithm.

BEZOUT'S IDENTITY FOR $\mathbb{Z}[i]$

Th^{m} / If $z, w \in \mathbb{Z}[i]$, not both zero, then there exist $m, n \in \mathbb{Z}[i]$ such that $zm + wn = \gcd(z, w)$

Proof: Calculate $\gcd(z,w)$ by Euclid's algo. in $\mathbb{Z}[i]$ then rearrange terms to discover Bezout's Identity. // [this was proof in $\mathbb{Z}$ also]

Th^{m} (Prime Divisor Property for Gaussian Integers) If a Gaussian prime $\bar{\omega} \mid \alpha\beta$ then $\bar{\omega} \mid \alpha$ or $\bar{\omega} \mid \beta$.

Proof: Suppose $\bar{\omega} \mid \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ where $\bar{\omega}$ is Gaussian prime. If $\bar{\omega} \nmid \alpha$ then it remains to show $\bar{\omega} \mid \beta$. Bezout's identity $\Rightarrow \exists m, n \in \mathbb{Z}[i]$ for which $\alpha m + \bar{\omega} n = \gcd(\alpha, \bar{\omega})$ thus $\alpha\beta m + \bar{\omega}\beta n = \beta \gcd(\alpha, \bar{\omega})$. Since $\bar{\omega} \mid \alpha\beta$ we have $\exists \gamma \in \mathbb{Z}[i]$ such that $\alpha\beta = \gamma\bar{\omega}$ thus, $m\gamma\bar{\omega} + \bar{\omega}\beta n = \beta \gcd(\alpha, \bar{\omega})$. We find $\gcd(\alpha, \bar{\omega})\beta = (m\gamma + n\beta)\bar{\omega}$. You can show (PROBLEM 85) that $\gcd(\alpha, \bar{\omega}) = \pm 1, \pm i$. Thus $\beta = \underbrace{(\pm 1, \pm i)(m\gamma + n\beta)}_{\text{some factor in } \mathbb{Z}[i]}\bar{\omega}$ thus $\bar{\omega} \mid \beta$ and the proof is done. //

Proof ↓ (see pg. ⑥ of LECTURE 2)

Th^{m} (Unique Prime Factorization) $z \in \mathbb{Z}[i] \Rightarrow z = \bar{\omega}_1 \bar{\omega}_2 \cdots \bar{\omega}_r$ for unique ~~primes~~ Gaussian primes $\bar{\omega}_1, \ldots, \bar{\omega}_r$ (upto reordering and $\pm 1, \pm i$).

Remark: I've said a bit more about how the proofs in $\mathbb{Z}$ lift to proofs in $\mathbb{Z}[i]$ than Stillwell. I hope you can see he is justified in this omission. If we trust in his assertion we can still make the main arguments in §6.5, 6.6, 6.7 w/o trouble.

In §6.3 we saw a prime p which was real was not of the form $p = a^2+b^2$. Likewise a pure imaginary prime of form $p = iq \Rightarrow q$ is real Gaussian prime $\Rightarrow iq \neq i(a^2+b^2)$. We argued if $p = a^2+b^2$ was an ordinary prime in $\mathbb{Z}$ then $p = (a+ib)(a-ib)$ where norm $(a \pm ib) = p$ thus $a \pm ib$ we seen to be Gaussian primes. We now continue the story:

Th^{m}/ Gaussian primes $a+ib$ with $a, b \neq 0$ give $p = a^2+b^2$ prime in $\mathbb{Z}$.

Proof: we argued in Lecture 10 that $a+ib$ a Gaussian prime $\Rightarrow a-ib$ also a Gaussian prime. Observe $(a+ib)(a-ib) = a^2+b^2$. Set $p = a^2+b^2$ and observe $p \in \mathbb{N}$. If $p = rs$ for $1 < r, s < p$ then $(a+ib)(a-ib) = rs = p$. But p has factorization $\overline{\omega}_1 = a+ib$, $\overline{\omega}_2 = a-ib$ both Gaussian primes with $a, b \neq 0$ thus $\overline{\omega}_1, \overline{\omega}_2$ do not match rs factorization which either is a pair of real Gaussian primes or splits $r = (\gamma+\delta i)(\gamma-\delta i)$, $s = (c_1+ic_2)(c_1-ic_2)$ which makes p formed either by 2 real factors or 4 complex Gaussian primes. Both cases violate the known factorization $p = (a+ib)(a-ib)$ hence $\nexists r, s$ primes for which $p = rs$ $\therefore$ p is prime in $\mathbb{Z}$. Moreover, $p = |a|^2+|b|^2$ for the unique $|a|, |b| \in \mathbb{N}$ given $a+ib$. //

(note: this improves my original pg. 10 of Lecture 10)

§6.5 Fermat's two square theorem

- primes of form $4\mathbb{Z}+3$ not of form a^2+b^2.
- fermat's 2-square theorem says the remaining odd primes of form $4\mathbb{Z}+1$ are of the form a^2+b^2!
- Outline: factor $p = 4n+1$ with help of $m \in \mathbb{Z}$ for which $p = m^2+1$. We find this m via Wilson's Th^m

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv -1 \pmod{p}$$

Lagrange's Lemma:
A prime $p = 4n+1$ divides m^2+1 for some $m \in \mathbb{Z}$

Proof: apply Wilson's ~~Lemma~~ Th^m to prime $p = 4n+1$

$$\begin{aligned} -1 &\equiv 1 \times 2 \times 3 \times \cdots \times 4n \pmod{p} \\ &\equiv (1 \times 2 \cdots \times 2n) \times (2n+1) \times \cdots \times (4n) \pmod{p} \\ &\equiv (1 \cdot 2 \cdots 2n) \times (-2n) \times \cdots \times (-1) \pmod{p} \quad (4n \equiv -1 \bmod p) \text{ etc..} \\ &\equiv (1 \cdot 2 \cdots \cdot 2n)^2 (-1)^{2n} \pmod{p} \\ &= [(2n)!]^2 \pmod{p}. \end{aligned}$$

Hence $m = (2n)!$ gives $m^2 \equiv -1 \bmod p$
and we conclude $p \mid m^2+1$. //

Fermat's two square theorem: Let $n \in \mathbb{N}$ as usual. If $p = 4n+1$ is prime then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Proof: If $p = 4n+1$ is prime then Lagranges Lemma $\Rightarrow \exists m \in \mathbb{Z}$ for which $p \mid m^2+1$. Thus $p \mid (m+i)(m-i)$. Observe $p \mid (m \pm i) \Rightarrow \exists q \in \mathbb{Z}[i]$ such that $m \pm i = pq$

Divide by $p \neq 0$ to obtain $\frac{m \pm i}{p} = q$. Clearly ~~$\frac{1}{p} \notin \mathbb{Z}[i]$~~ hence $\frac{m \pm i}{p} = q \notin \mathbb{Z}[i] \therefore p \nmid (m \pm i)$.

This shows $p \mid (m+i)(m-i)$ yet $p \nmid m+i$ and $p \nmid m-i$ hence p does not satisfy Gaussian Prime Divisor Prop and we deduce p is not a Gaussian prime. It follows p is an ordinary prime of form $p = a^2+b^2$

from §6.3 if we forgot: pg. 105 Stillwell (our Lecture 10)

"REAL GAUSSIAN PRIMES: AN ORDINARY PRIME $p \in \mathbb{N}$ IS A GAUSSIAN PRIME $\Leftrightarrow$ $p \neq a^2+b^2$"

§6.6 PYTHAGOREAN TRIPLES

In Lecture 1 or §1.8 we studied $x^2+y^2=z^2$ by glibly using $\mathbb{Z}[i]$. We now return to carefully evaluate those arguments in view of the theory from Chapter 6.

~

Consider that:

$$(2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1 \equiv 1 \bmod 4$$
$$(2k)^2 = 4k^2 \equiv 0 \bmod 4.$$

Also, consider,

$$(2j+1)^2+(2k+1)^2 = 4j^2+4j+1+4k^2+4k+1$$
$$= 4(j^2+j+k^2+k)+2 \equiv 2 \bmod 4$$

$\Rightarrow$ sum of odd squares is <u>not</u> a square!

Sol^n (x,y,z) to $x^2+y^2=z^2$ is called <u>primitive</u> if $\nexists$ common factor of x,y,z (except ± 1). Since $x,y,z \in \mathbb{Z} = 2\mathbb{Z} \cup (2\mathbb{Z}+1)$ we have the following:

> <u>Claim</u>: In primitive triple (x,y,z) one of x,y is even and z is odd. $\left[(\text{even})^2+(\text{odd})^2=(\text{odd})^2\right]$

Our argument from §1.8,

$$x^2+y^2=z^2 \Rightarrow \underbrace{(x+iy)(x-iy)}_{\text{Gaussian prime factors of } z^2} = z^2$$

We <u>CONJECTURED</u> (like Lagrange or Euler in late 18th century)

1.) If $\gcd(x,y)=1$ then $x+iy$, $x-iy$ are likewise relatively prime in $\mathbb{Z}[i]$

2.) In $\mathbb{Z}[i]$ the relatively prime factors of a square are squares

Again our conjectures were:

1.) $x, y \in \mathbb{Z}$ with $\gcd(x,y)=1 \Rightarrow \gcd(x+iy, x-iy) = [1]$

2.) In $\mathbb{Z}[i]$, relatively prime factors of a square are squares.

To see 1. is correct, observe:

Proposition: If $\gcd(x,y)=1$ in $\mathbb{Z}$ then $\gcd(x,y)=1$ in $\mathbb{Z}[i]$ (for $x, y \in \mathbb{Z}$)

Proof: Since $x, y \in \mathbb{Z}$ any common divisor $\alpha \in \mathbb{Z}[i]$ must also allow $\bar{\alpha} \in \mathbb{Z}[i]$ as common divisor. That is $\alpha | x$ and $\alpha | y \Rightarrow \bar{\alpha} | x$ and $\bar{\alpha} | y$ thus $\alpha\bar{\alpha} | x$ and $\alpha\bar{\alpha} | y$ where $\alpha\bar{\alpha} = n \in \mathbb{N}$ with $n \geq 2$. * (nice question!)

Next, observe $2x = (x+iy) - (x-iy)$ and $2yi = (x+iy) - (x-iy)$ thus a common divisor $\alpha \in \mathbb{Z}[i]$ of $\alpha | x+iy$ and $\alpha | x-iy$ has $\alpha | 2yi$ and $\alpha | 2x$.

But, $\gcd(x,y)=1 \Rightarrow$ common prime divisor $\alpha = \pm 1 \pm i$ (Gaussian)

(ordinary ~~prime~~ real Gaussian prime case disallowed by fact $x, y \in \mathbb{Z}$ share no prime factors in $\mathbb{Z}$)

However, if $\exists \alpha = \pm 1 \pm i$ a divisor of $x+iy$ & $x-iy$ then $(x+iy)(x-iy) = (1+i)\gamma\,(1-i)\bar{\gamma} = 2\gamma\bar{\gamma}$ etc.

$\Rightarrow x^2+y^2$ is even (which is false for primitive triple see pg. (7) if forgot) //

The statement of 2 needs a little modification

2.) In $\mathbb{Z}[i]$, relatively prime factors of a square are squares, up to unit-factors

Remark: we had a hwk problem $\approx$ about the $\pm$ issue in $\mathbb{Z}$

Observe $x+iy$ and $x-iy$ have no common Gaussian prime factor, however considering $x^2+y^2=z^2$ we see each Gprime factor of z occurs in even power.

$$(x+iy)(x-iy) = z^2 = \overline{w}_1^{\,2}\,\overline{w}_2^{\,2}\cdots\overline{w}_r^{\,2}$$

$$\Rightarrow x+iy = \overline{w}_{i_1}^{\,2}\,\overline{w}_{i_2}^{\,2}\cdots\overline{w}_{i_r}^{\,2}\,(\pm 1, \pm i)$$

$$\& \quad x-iy = \overline{w}_{j_1}^{\,2}\,\overline{w}_{j_2}^{\,2}\cdots\overline{w}_{j_r}^{\,2}\,(\pm 1, \pm i)$$

Th^{n}/ $x \pm iy$ are products of squares of Gaussian primes and possibly one of $1, -1, i$ or $-i$

Now we can be explicit! We have $x-iy$ of the form:

$$\left.\begin{aligned} (s-ti)^2 &= s^2 - 2sti - t^2 = (s^2-t^2) - 2sti \\ -(s-ti)^2 &= -s^2 + 2sti + t^2 = (t^2-s^2) + 2sti \\ i(s-ti)^2 &= 2st + (s^2-t^2)i \\ -i(s-ti)^2 &= -2st + (t^2-s^2)i \end{aligned}\right\} \text{ for some } s,t \in \mathbb{Z}$$

Consequently, we find $x^2+y^2=z^2$ has primitive sol^{n} with x, y of the form u^2-v^2 & $2uv$ for some $u, v \in \mathbb{N}$

Remark: inclusion of the units $\pm 1, \pm i$ gives us formulas which treat x & y symmetrically. This is to be expected given the structure of $x^2+y^2=z^2$ where $x \longleftrightarrow y$

Thus, $x^2+y^2 = (u^2-v^2)^2 + (2uv)^2 = (u^2+v^2)^2 = z^2$ thus:

Comment: The primes which are sums of squares are those who appear as hypotenuses of right-angled triangles with integer sides

§6.7 PRIMES OF THE FORM $4n+1$

We prove $\exists$ ∞ly many primes of the form $4n+1$. Exercises 6.3.4, 6.3.5, 6.3.6 served to show $\exists$ ∞ly many primes of form $4n+3$.

Th^m/"Quadratic character of -1." The congruence $x^2 \equiv -1 \pmod{p}$ where p is an odd prime, has a sol^n precisely when $p = 4n+1$

Proof: when $p = 4n+1$, Lagrange's Lemma gives us $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$. (we used "n" in the Lemma but that's just notation!). Odd primes $2\mathbb{Z}+1 = (4\mathbb{Z}+1) \cup (4\mathbb{Z}+3)$ we've already covered $4\mathbb{Z}+1$ case, now consider $p = 4n+3$.

Suppose (towards $\nrightarrow\leftarrow$) that $\exists x \in \mathbb{Z}$ for which

$$x^2 \equiv -1 \pmod{p = 4n+3}$$

Raise both sides to the $2n+1$ power,

$$(x^2)^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{p = 4n+3}$$

However, $4n+2 = p-1$ hence Fermat's little theorem tells us $x^{4n+2} = x^{p-1} \equiv 1 \pmod{p}$ yet

$$x^{4n+2} \equiv -1 \pmod{p}$$

Which is a contradiction $\therefore$ $x^2 \equiv -1 \pmod{p = 4n+3}$ has no sol^n and the theorem follows. //

Comment: the odd primes p that divide values of x^2+1, for $x \in \mathbb{Z}$, are precisely the primes of form $p = 4n+1$.

Remark: I plan to give (optional!) handout from Shifrin's text. In that section he explores various quotients of $\mathbb{Z}[i]$ and exploits the geometry of the integer lattice in $\mathbb{C}$. Also his proofs of the items in §6.3–6.7 are rather efficient. That said, some Math422 is needed for context of the handout so I mainly give it as a 422 tease. ☺

Th^{m} / Infinitude of primes of form $4n+1$:
$\exists$ ∞ly many primes of form $p = 4n+1$

Proof: given $x^2+1 \equiv 0 \bmod p$ has sol^{n} precisely when $p = 4n+1$
@(prime p assumed) it suffices to show ∞ly many primes divide values of x^2+1 for $x \in \mathbb{Z}$. Proceed by $\rightarrow\leftarrow$
$\S$ $\exists$ finitely many primes $p_1, p_2, \ldots, p_n$ which divide values of x^2+1 for $x \in \mathbb{Z}$.

Continuing to follow Stillwell essentially word for word/
Consider the polynomial

$$g(y) = (p_1 p_2 \cdots p_n y)^2 + 1$$

If $p \mid g(y)$ for $y \in \mathbb{Z}$ then $p \mid x^2+1$ with $x = p_1 p_2 \cdots p_n y$.
However, $p_1, p_2, \ldots, p_n \nmid g(y)$ as each leaves remainder 1.
Thus, no prime divides $g(y)$ for any $y \in \mathbb{Z}$ (we're assuming $p_1, p_2, \ldots, p_n$ are only primes which divide x^2+1)
Thus, $g(y) = \pm 1$ <u>for all $y \in \mathbb{Z}$</u>. That is, *

$$(p_1 p_2 \cdots p_n y)^2 + 1 = \pm 1$$

Of course the quadratic eq^{n}'s

$$(p_1 p_2 \cdots p_n)^2 y^2 + 1 = 1 \quad \& \quad (p_1 p_2 \cdots p_n)^2 y^2 + 1 = -1$$

have at most two sol^{n}'s, a clear $\rightarrow\leftarrow$ to claim *
Thus x^2+1 is divisible by ∞ly many primes
and so $\exists$ ∞ly many primes of form $4n+1$. //

Comment: it follows $\exists$ ∞ly many primes of form a^2+b^2
$\therefore$ $\exists$ ∞ly many non-red, non-pure-imaginary Gaussian primes stemming from $a^2+b^2 = (a+ib)(a-ib)$.

§6.8 Discussion:

- Our proof for fermat's 2-square thm is due to Dedekind from around 1894. The original proof (unwritten, undocumented) was claimed to be by descent by Fermat. The argument goes roughly like this: if $\exists$ one prime of form $4n+1$ but not the sum of squares then $\exists$ only many smaller such primes (absurd.) Later (1755) Euler actually published such a proof resulting from several years effort.
- Lagrange's Lemma (1773) was key to simplifying the proof, $\mathbb{Z}[i]$ came later, only completely cleaned-up much later by Dedekind (1894).
- Minkowski's geometry of #'s offers an alternative proof $\approx$ 1890's
- 4 square identity Euler 1748
- 4 square theorem of Lagrange: every $n \in \mathbb{N}$ is sum of at most four natural # squares.
  - $\hookrightarrow$ based on Lemma any prime $p \mid l^2+m^2+1$ for some m, l.
- Proof of 2-square identity as seen from $\mathbb{Z}[i]$ is a proof from a natural structure
- Likewise the 4-square identity proof from quaternion integers will be seen in Chapter 8. Central to argument the multiplicative prop. of quaternion norm, just like the importance we saw for $\mathbb{Z}[i]$ norm in this chapter.

§6.8 Discussion Continued:

Another direction to generalize our study of x^2+y^2 and correspondingly $\mathbb{Z}[\sqrt{-1}]$ is to consider x^2+2y^2 or x^2+3y^2 to which the structure of $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{-3}]$ prove useful. In next chapter we find (as did Fermat some time ago w/o the benefit of modern algebra) p a prime,

$$p = x^2 + 2y^2 \iff p = 8n+1 \text{ or } p = 8n+3$$

$$p = x^2 + 3y^2 \iff p = 3n+1$$

$\exists$ natural analogs of our 2-square thm proof to obtain the results above by manipulation of $a+b\sqrt{-2}$ or $c+d\sqrt{-3}$ numbers.

- Lagrange's Lemma also adapts:

this chapter: if $p = 4n+1$ then $p \mid m^2+1$ for some $m \in \mathbb{Z}$.
(tied to quadratic character at -1)

that is; -1 is congruent to a square mod p precisely when $p = 4n+1$.

For 2-square thm concerning x^2+2y^2, x^2+3y^2 we need to know about the quadratic characters of -2 and -3. It turns out that:

$$-2 \equiv \text{square mod } p \iff p = 8n+1 \text{ or } 8n+3$$

$$-3 \equiv \text{square mod } p \iff p = 3n+1$$

It turns out there is a sweeping general method to determine these quadratic characters. Noticed by Euler in study of x^2+y^2, x^2+2y^2, x^2+3y^2 etc... then proved by Gauss (1801) the machine of Quadratic Reciprocity
- (our Chapter 9) -