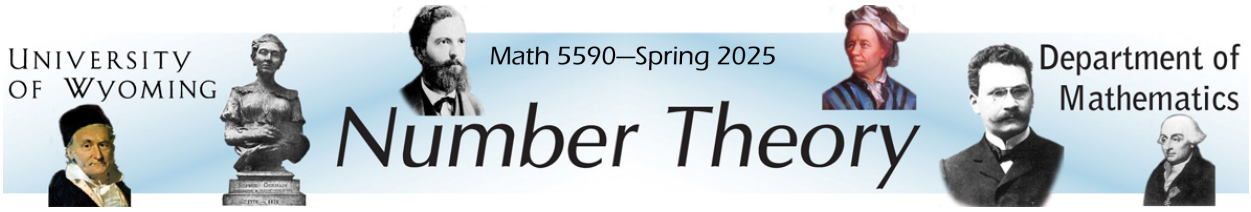

HW1

(Due Monday, March 10, 2025)

Instructions: See the course syllabus for general expectations regarding homework. Submit your solutions through WyoCourses.

1. What is the probability that two large 'randomly chosen' large integers m, n have the property that $\gcd(m,n) = 2$? The question should be interpreted as follows: Determine the value of
$$\lim_{N\to\infty} \frac{\big|\{(m,n) \in [1,N]^2 \,:\, \gcd(m,n) = 2\}\big|}{N^2},$$
given that the limit exists.

In the following, $K = \mathbb{Q}[\sqrt{-5}] \supset \mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. In place of the notation $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots$ used in class for prime ideals in $\mathcal{O}$, I will try a more systematic notation $\mathfrak{p}_p$ for a prime ideal lying above the rational prime p (i.e. $\mathfrak{p}_p \cap \mathbb{Z} = p\mathbb{Z}$; $\mathfrak{p}_p$ is a prime ideal dividing $p\mathcal{O}$). Although I am using lower case Fraktur fonts, feel free to use calligraphic fonts $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$, ... or whatever works best for you. (I used the calligraphic font for $\mathcal{O}$ in place of the ever-popular upper or lower case Fraktur $\mathfrak{O}$, $\mathfrak{o}$.) The Dedekind zeta function of this extension is

$$\begin{aligned}\zeta_K(s) &= \sum_{0\neq\mathfrak{a}\subset\mathcal{O}} \frac{1}{N(\mathfrak{a})^s} = \prod_{0\neq\mathfrak{p}\subset\mathcal{O}} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \\ &= \frac{1}{1-\frac{1}{2^s}} \cdot \frac{1}{1-\frac{1}{5^s}} \cdot \prod_{\substack{p\equiv 1,3,7,9 \\ \text{mod } 20}} \Big(\frac{1}{1-\frac{1}{p^s}}\Big)^2 \cdot \prod_{\substack{p\equiv 11,13,17,19 \\ \text{mod } 20}} \frac{1}{1-\frac{1}{p^{2s}}}\end{aligned}$$

where $\mathfrak{a}$ ranges over all nonzero ideals of $\mathcal{O}$; and $\mathfrak{p}$ ranges over all nonzero prime ideals of $\mathcal{O}$; p ranges over rational primes. This means that for every rational prime p, the prime ideal $p\mathbb{Z} \subset \mathbb{Z}$ factorizes in $\mathcal{O}$ as follows:

- 2 and 5 ramify as $2\mathcal{O} = \mathfrak{p}_2^2 = (2, 1+\sqrt{-5})^2$, $5\mathcal{O} = \mathfrak{p}_5^2 = (\sqrt{-5})^2$. In each of these cases, the residue ring has structure $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p[x]/(x^2) \cong \mathbb{F}_p[\varepsilon]$ where $\varepsilon^2 = 0$ (the ring of 'dual numbers' over $\mathbb{F}_p$).
- For $p \equiv 1, 3, 7$ or $9 \bmod 20$, p splits as $p\mathcal{O} = \mathfrak{p}_p\overline{\mathfrak{p}_p}$. In each of these cases, the residue ring $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p \oplus \mathbb{F}_p$. For example, $3\mathcal{O} = \mathfrak{p}_3\overline{\mathfrak{p}_3} = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ and $7\mathcal{O} = \mathfrak{p}_7\overline{\mathfrak{p}_7} = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$.

- For $p \equiv 11, 13, 17$ or $19 \mod 20$, p remains prime, i.e. the ideal $p\mathcal{O} \subset \mathcal{O}$ is prime (and maximal) and the residue field $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^2}$. (I could write $11\mathcal{O} = \mathfrak{p}_{11}$, and similarly for other primes p in these congruence classes; but then I would have two different names for the same ideal, which I don't really need.)

Recall that an element $\alpha = a+b\sqrt{-5} \in \mathcal{O}$ has norm $N(\alpha) = \alpha\overline{\alpha} = a^2+5b^2$; whereas an ideal $\mathfrak{a} \subseteq \mathcal{O}$ has norm $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. Both maps are multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$, and $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. For a principal ideal $(\alpha) = \alpha\mathcal{O}$, the notions coincide: $N((\alpha)) = |N(\alpha)|$. (The absolute value is required for general rings of integers, although in this case it is superfluous.) The latter identity follows from properties of more general integer lattices, as follows. Multiplication by α gives a surjective $\mathbb{Z}$-module homomorphism $m_\alpha : \mathcal{O} \to (\alpha)$, $v \mapsto \alpha v$ whose matrix (with respect to the basis $\{1, \sqrt{-5}\}$) is $\left[\begin{smallmatrix} a & -5b \\ b & a \end{smallmatrix}\right]$, whose determinant gives the area of a fundamental parallelogram in (α). This determinant, namely $N((\alpha)) = |\mathcal{O}/(\alpha)| = a^2+5b^2 = |N(\alpha)|$, equals the number of points of the lattice $\mathcal{O}$ in each shift of the fundamental parallelogram for (α); and this is the index of (α) in $\mathcal{O}$.

2. How many *ideals* $\mathfrak{a} \subset \mathcal{O}$ are there of norm 120? How many *elements* $\alpha \in \mathcal{O}$ are there of norm 120?

3. In the prime factorization $23\mathcal{O} = \mathfrak{p}_{23}\overline{\mathfrak{p}_{23}}$, find the prime ideals $\mathfrak{p}_{23}$, $\overline{\mathfrak{p}_{23}}$ explicitly.

In preparation for problem #4,5 below, let us demonstrate how to factorize the principal ideal $\mathfrak{b} = (11+\sqrt{-5})$, whose norm is simply the norm of its generator:

$$N(\mathfrak{b}) = |N(11+\sqrt{-5})| = (11+\sqrt{-5})(11-\sqrt{-5}) = 126 = 2 \cdot 3^2 \cdot 7.$$

There is a unique prime ideal $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ of norm 2, so this must divide $\mathfrak{b}$. Also $\mathfrak{b}$ must be divisible by either $\mathfrak{p}_7 = (7, 3+\sqrt{-5})$ or $\overline{\mathfrak{p}_7} = (7, 3-\sqrt{-5})$. Furthermore, $\mathfrak{b}$ has two factors of norm 3, both of which are either $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$ or $\overline{\mathfrak{p}_3} = (3, 1-\sqrt{-5})$. Now $\mathfrak{b}$ must be divisible by either $\mathfrak{p}_3^2$ or $\overline{\mathfrak{p}_3}^2$ (since it is obviously not divisible by $\mathfrak{p}_3\overline{\mathfrak{p}_3} = (3)$). This show that $\mathfrak{b}$ has one of four possible factorizations:

$$\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_7\,, \quad \mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}_7}\,, \quad \mathfrak{p}_2\overline{\mathfrak{p}_3}^2\mathfrak{p}_7\,, \quad \text{or} \quad \mathfrak{p}_2\overline{\mathfrak{p}_3}^2\overline{\mathfrak{p}_7}\,.$$

To see which one is the correct factorization of $\mathfrak{b}$, let's use the identities

$$\text{(i)} \quad \mathfrak{p}_2\mathfrak{p}_7 = (3+\sqrt{-5}), \quad \mathfrak{p}_2\overline{\mathfrak{p}_7} = (3-\sqrt{-5}).$$
$$\text{(ii)} \quad \mathfrak{p}_3^2 = (2-\sqrt{-5}), \quad \overline{\mathfrak{p}_3}^2 = (2+\sqrt{-5}); \quad \text{and}$$

These are similar to the identities $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5})$ and $\mathfrak{p}_2\overline{\mathfrak{p}_3} = (1-\sqrt{-5})$ discussed in class. Let's give a more detailed explanation of (i) here; we leave (ii) for you to do. In each case, we have the product of an even number of non-principal ideals, which must be principal, since $h_K = 2$. And in each case, we know the norm of the ideal, which is simply

the norm of its generator. This information is often enough to determine the ideal, at least up to conjugacy. For example, $\mathfrak{p}_2\mathfrak{p}_7 = (3+\sqrt{-5})$ or $(3-\sqrt{-5})$ since the only solutions of $a^2+5b^2 = 14$ are $(\pm 3, \pm 1)$, and $(-\alpha) = (\alpha)$. If $\mathfrak{p}_2\mathfrak{p}_7 = (3-\sqrt{-5})$, then

$$\begin{aligned} 2(3+\sqrt{-5}) &\subseteq \mathfrak{p}_2\mathfrak{p}_7 = (3-\sqrt{-5}) \\ 2(2+3\sqrt{-5}) = 2(3+\sqrt{-5})^2 &\subseteq (3+\sqrt{-5})(3-\sqrt{-5}) = (14) \\ (2+3\sqrt{-5}) &\subseteq (7) \end{aligned}$$

If this were correct, then by comparing norms, we would have equality, and this would be a contradiction. (The only units in $\mathcal{O}$ are ± 1, and we cannot have $2+3\sqrt{-5} = \pm 7$.) So we must have $\mathfrak{p}_2\mathfrak{p}_7 = (3+\sqrt{-5})$ as claimed. The second part of (i) follows by conjugating the first part.

An alternative proof of (i) involves showing containment in either direction. We have

$$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_7 &\subseteq \big(2\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}\big)\big(7\mathbb{Z} + (3+\sqrt{-5})\mathbb{Z}\big) \\ &\subseteq 14\mathbb{Z} + 7(1+\sqrt{-5})\mathbb{Z} + (3+\sqrt{-5})\mathbb{Z} \\ &= (3+\sqrt{-5})\big[(3-\sqrt{-5})\mathbb{Z} + (4+\sqrt{-5})\mathbb{Z} + \mathbb{Z}\big] \;=\; (3+\sqrt{-5})\mathbb{Z} \end{aligned}$$

and the reverse inclusion follows from

$$3+\sqrt{-5} = (1+\sqrt{-5})\big[7 - (3+\sqrt{-5})\big] - 2(3+\sqrt{-5}) \in \mathfrak{p}_2\mathfrak{p}_7.$$

Getting both directions of this inclusion can be a little tricky; but as we observed in class, you only need to verify inclusion in one direction since the two ideals in question have the same norm. (The argument is as follows: Suppose $\mathfrak{a} \supseteq \mathfrak{b}$ and both ideals have the same norm. Then $|\mathfrak{a}/\mathfrak{b}| = \left|\frac{\mathcal{O}/\mathfrak{b}}{\mathcal{O}/\mathfrak{a}}\right| = \frac{N(\mathfrak{b})}{N(\mathfrak{a})} = 1$, so $\mathfrak{a} = \mathfrak{b}$.) Still, I'd say the previous argument for proving (i) is easier.

4. Prove that $\mathfrak{p}_3^2 = (2-\sqrt{-5})$ as claimed in (ii) above. (And so by conjugation, the other assertion of (ii) follows.)

By considering all four possible pairs from (i) and (ii) above, we obtain the correct prime factorization

$$\mathfrak{b} = (11+\sqrt{-5}) = (3-\sqrt{-5})(2+\sqrt{-5}) = \mathfrak{p}_2\overline{\mathfrak{p}_3}^2\overline{\mathfrak{p}_7}\,.$$

5. Find the prime factorization of the principal ideal $(1+5\sqrt{-5})$ into prime ideals in $\mathcal{O}$.

Refer to the pre-recorded lecture of Feb 19.

6. Using appropriate software, use the continued fraction expansion of $\sqrt{61}$ to find the fundamental solution (the smallest nontrivial positive integer solution) of $x^2-61y^2 = 1$.