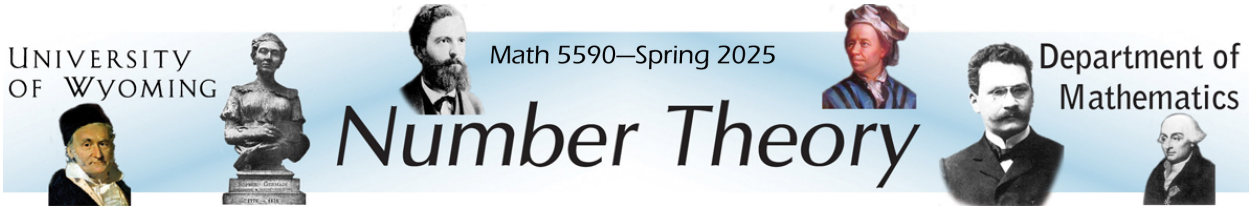

Solutions to HW1

1. The required probability is $\frac{1}{4\zeta(2)} = \frac{3}{2\pi^2}$ (about 15.2%). Given two large randomly (and independently) chosen integers m, n, let E be the event that $\gcd(m,n) = 2$, and let E' be the event that $\gcd(m,n) = 2$. Then E' implies E. We have $Pr(E) = \frac{1}{4}$. The conditional probability $Pr(E' \,|\, E) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$ since if E holds, then $m = 2m'$ and $n = 2n'$ where m', n' are two large randomly (and independently) distributed large integers; and $\gcd(m,n) = 2$ iff $\gcd(m,n) = 1$. This gives

$$Pr(E') = Pr(E' \,|\, E)Pr(E) + Pr(E' \,|\, E^c)Pr(E^c) = \tfrac{1}{\zeta(2)} \cdot \tfrac{1}{4} + 0 \cdot \tfrac{3}{4} = \tfrac{1}{4\zeta(2)} = \tfrac{3}{2\pi^2}$$

where E^c is the complement of E (the event that m and n are *not* both even).

Alternatively, the probability that $\gcd(m,n) = 2$ is

$$\begin{aligned} & Pr(m,n \text{ congruent to } 2,2 \text{ or } 2,0 \text{ or } 0,2 \bmod 4) \\ & \quad \times Pr(m,n \text{ not both divisible by } 3) \\ & \quad \times Pr(m,n \text{ not both divisible by } 5) \\ & \quad \times Pr(m,n \text{ not both divisible by } 7) \\ & \quad \times Pr(m,n \text{ not both divisible by } 11) \times \text{ etc.} \\ = \tfrac{3}{16} \prod_{p \text{ odd}} (1 - \tfrac{1}{p^2}) & = \tfrac{1}{4} \prod_{p} (1 - \tfrac{1}{p^2}) = \tfrac{1}{4\zeta(2)} = \tfrac{3}{2\pi^2}. \end{aligned}$$

2. There are exactly two ideals $\mathfrak{a} \subset \mathcal{O}$ of norm 120. This can be read off from the coefficient 2 of the term $\frac{1}{120^s}$ in

$$\begin{aligned} \zeta_K(s) &= \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}} \frac{1}{N(\mathfrak{a})^s} \\ &= \left(1 + \tfrac{1}{2^s} + \tfrac{1}{4^s} + \tfrac{1}{8^s} + \cdots\right)\left(1 + \tfrac{2}{3^s} + \tfrac{3}{9^s} + \tfrac{4}{27^s} + \cdots\right)\left(1 + \tfrac{1}{5^s} + \tfrac{1}{25^s} + \tfrac{1}{125^s} + \cdots\right) \times \cdots \\ &= 1 + \tfrac{1}{2^s} + \tfrac{2}{3^s} + \tfrac{1}{4^s} + \cdots + \tfrac{2}{120^s} + \cdots. \end{aligned}$$

Alternatively, the only two ideals of norm 120 in $\mathcal{O}$ are $\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5 = (10{-}2\sqrt{-5})$ and $\mathfrak{p}_2^3\overline{\mathfrak{p}_3}\mathfrak{p}_5 = (10{+}2\sqrt{-5})$. There are four elements $\pm 10 \pm 2\sqrt{-5}$ of norm 120 in $\mathcal{O}$ since each of the ideals of norm 120 is principal and has two different choices of generator (arising from the two different choices of unit $\pm 1 \in \mathcal{O}$). Alternatively, elementary considerations show that the only four integer solutions of $x^2{+}5y^2 = 120$ are $(\pm 10, \pm 2)$.

3. We take $\mathfrak{p}_{23} = (23, 8+\sqrt{-5})$, $\overline{\mathfrak{p}_{23}} = (23, 8-\sqrt{-5})$. As explained in class,

$$\begin{aligned}\mathcal{O}/23\mathcal{O} &\cong \mathbb{F}_{23}[\sqrt{-5}] \cong \mathbb{F}_{23}[x]/(x^2+5) \cong \mathbb{F}_{23}[x]/((x-8)(x+8)) \\ &\cong \mathbb{F}_{23}[x]/(x+8) \oplus \mathbb{F}_{23}[x]/(x-8) \cong \mathbb{Z}[x]/(23, x+8) \oplus \mathbb{Z}[x]/(23, x-8) \\ &\cong \mathcal{O}/\mathfrak{p}_{23} \oplus \mathcal{O}/\overline{\mathfrak{p}_{23}}\,.\end{aligned}$$

We used the fact that the roots of x^2+5 in $\mathbb{F}_{23}$ are ± 8. Note that both summands of the direct sum are isomorphic to $\mathbb{F}_{23}$. Under the epimorphism $\mathbb{Z}[x] \to \mathcal{O}$, $x \mapsto \sqrt{-5}$,

4. $\mathfrak{p}_3^2 = (3, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (9, 3(1+\sqrt{-5}), -4+2\sqrt{-5})$ contains

$$9 - 3(1+\sqrt{-5}) + (-4+2\sqrt{-5}) = 2-\sqrt{-5}$$

so $\mathfrak{p}_3^2 \supseteq (2-\sqrt{-5})$. But both these ideals have norm 9, so they must be equal: $\mathfrak{p}_3^2 = (2-\sqrt{-5})$. Conjugating this gives $\overline{\mathfrak{p}_3}^2 = (2+\sqrt{-5})^2$.

5. $(1+5\sqrt{-5}) = (2+\sqrt{-5})(3+\sqrt{-5}) = \overline{\mathfrak{p}_3}^2 \cdot \mathfrak{p}_2\mathfrak{p}_7 = \mathfrak{p}_2\overline{\mathfrak{p}_3}^2\mathfrak{p}_7$. Once again the norm is $126 = 2 \cdot 3^2 \cdot 7$, so we have only a short list of prime ideals of the required norms to check until we find the correct combination.

6. The continued fraction decomposition $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 4, 3, 1, 14}]$ gives the cconvergents

$$7,\ 8,\ \tfrac{39}{5},\ \tfrac{125}{16},\ \tfrac{164}{21},\ \tfrac{453}{58},\ \tfrac{1070}{137},\ \tfrac{1523}{195},\ \tfrac{5639}{722},\ \tfrac{24079}{3083},\ \tfrac{29718}{3805},\ \tfrac{440131}{56353},\ \tfrac{469849}{60158},\ \tfrac{2319527}{296985},\ \tfrac{7428430}{951113},$$

$$\tfrac{9747957}{1248098},\ \tfrac{26924344}{3447309},\ \tfrac{63596645}{8142716},\ \tfrac{90520989}{11590025},\ \tfrac{335159612}{42912791},\ \tfrac{1431159437}{183241189},\ \tfrac{1766319049}{226153980},\ \ldots$$

The 22nd convergent (the last one shown here) gives the fundamental solution of Pell's equation $x^2 - 61y^2 = 1$, namely $(x, y) = (1766319049, 226153980)$.

Alternatively, a solution of $N(x+y\sqrt{61}) = x^2 - 61y^2 = -1$ is given by the 11th convergent listed above. We expand

$$(29718 + 3805\sqrt{61})^2 = 1766319049 + 226153980\sqrt{61}$$

to obtain the desired solution of $N(x+y\sqrt{61}) = (-1)^2 = 1$.