

Problem Set #6: Sweet Sorrow

How lucky I am to have something that makes saying goodbye so hard.

Same conventions as always: D is a squarefree integer, $D \neq 1$, and $\mathcal{O}_D = \mathbf{Z}[\tau] = \mathbf{Z} + \mathbf{Z}\tau$, where $\tau = \sqrt{D}$ when $D \equiv 2, 3 \pmod{4}$, and $\tau = \frac{1+\sqrt{D}}{2}$ when $D \equiv 1 \pmod{4}$.

WHICH 'WITSCH IS WHICH?

0. Do not confuse our Rabinowitsch (Y.G.) with the originator of Rabinowitsch's trick (J.L.), used in proofs of Hilbert's Nullstellensatz. See

<https://mathoverflow.net/questions/416577/identity-of-j-l-rabinowitsch-of-rabinowitsch-trick>

SEIZING THE MEANS OF PRIME PRODUCTION

1. Use Rabinowitsch's Theorem to check that $\mathcal{O}_D$ is a UFD for $D = -7, -11, -19, -43, -67, -163$.
2.
 - a) If $D \equiv 2, 3 \pmod{4}$, then 2 ramifies in $\mathcal{O}_D$.
 - b) If $D \equiv 2, 3 \pmod{4}$ and $D < -2$, then there are no $\alpha \in \mathcal{O}_D$ with $N\alpha = 2$.
 - c) Conclude: If $D < -2$ and $D \equiv 2, 3 \pmod{4}$, then $2 \nmid h_D$, where $h_D := \#\text{Cl}(\mathcal{O}_D)$. In particular, $\mathcal{O}_D$ is not a UFD.
3.
 - a) Prove, using nothing more than the material on the first-year problem sets:
Whenever $p > 5$ is prime, there is a prime $q < p$ for which the Legendre symbol $\left(\frac{q}{p}\right) = 1$.
 - b) Take as known the Baker–Heegner–Stark theorem: The only squarefree $D < 0$ with $\mathcal{O}_D$ a UFD are $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Prove:
Whenever $p > 163$ is a prime with $p \equiv 3 \pmod{4}$, there is a prime $q < \sqrt{p/3}$ with $\left(\frac{q}{p}\right) = 1$.

Linnik and Vinogradov have shown the following: Fix $\epsilon > 0$. There is a constant $p_0(\epsilon)$ such that: Whenever p is a prime exceeding $p_0(\epsilon)$, there is a prime $q < p^{\frac{1}{4}+\epsilon}$ with $\left(\frac{q}{p}\right) = 1$. It would be of substantial interest to replace the constant $\frac{1}{4}$ appearing in the exponent by anything smaller.

EULER VS HARDY AND LITTLEWOOD

In 1923, Hardy and Littlewood proposed the following generalization of the twin prime conjecture, known as the prime tuples conjecture.

Let $a_1, a_2, \dots, a_k$ be a sequence of integers such that, for every prime p , there is at least one residue class mod p missing from the list

$$a_1 \bmod p, \quad a_2 \bmod p, \quad \dots, \quad a_k \bmod p.$$

Then there are infinitely many positive integers n for which

$$n + a_1, \quad n + a_2, \quad \dots, \quad n + a_k \quad \text{are simultaneously prime.}$$

4. (Granville) Assume the tuples conjecture. Show that for every $B \in \mathbf{Z}^+$, there is an $A \in \mathbf{Z}^+$ with the property that

$$n^2 - n + A \quad \text{is prime for every integer } 0 < n < B.$$

Hence: Assuming the tuples conjecture, there is a polynomial $n^2 - n + A$ which generates primes for all $n = 1, 2, 3, \dots, 2026$.

STRETCHING: THE TRUTH ABOUT NON-UNIQUE FACTORIZATION

The next four problems walk you through a proof of the theorem of Narkiewicz, Steffan, Valenza determining the elasticity of the rings $\mathcal{O}_D$. For all of these exercises, assume Landau's theorem that each ideal class in $\mathcal{O}_D$ is represented by a prime ideal.

5. Show that $\rho_D \geq \frac{1}{2} \text{Dav Cl}(\mathcal{O}_D)$.

Adapt the proof from lecture that $\rho_D > 1$ whenever $h_D > 2$.

6. (Davenport) The width $w(\alpha)$ of a nonzero $\alpha \in \mathcal{O}_D$ is the number of prime ideals appearing (with multiplicity) in the prime ideal factorization of (α) . For instance, the width of 6 in $\mathbf{Z}[i]$ is 3, since $(6) = (1 + i)(1 - i)(3)$.

Show that

$$\max_{\pi} w(\pi) = \text{Dav Cl}(\mathcal{O}_D),$$

where the maximum is taken over all irreducible elements π of $\mathcal{O}_D$.

7. Suppose that $\alpha \in \mathcal{O}_D$ is a nonunit for which

$$\alpha = \pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell,$$

where each π_i, ρ_j is irreducible in $\mathcal{O}_D$ and $k \leq \ell$. Assume none of the π_i and ρ_j are prime. Prove:

- The width of α is at least 2ℓ .
 - The width of α is at most $k \text{Dav Cl}(\mathcal{O}_D)$.
8. (Narkiewicz–Steffan–Valenza) If $h_D > 1$, then $\rho_D = \frac{1}{2} \text{Dav Cl}(\mathcal{O}_D)$.
9. In this problem we work in the ring $\mathbf{Z}[5i]$ (note that this is **not** an $\mathcal{O}_D$!). For each nonzero nonunit $\alpha \in \mathbf{Z}[5i]$, put

$$\rho(\alpha) = \frac{\text{max length of an irred. factorization of } \alpha}{\text{min length of an irred. factorization of } \alpha}.$$

- 5 is irreducible in $\mathbf{Z}[5i]$.
- For every $k \in \mathbf{Z}^+$, both $5(2 + i)^k$ and $5(2 - i)^k$ are irreducible.
- $\rho(5^{k+2}) \geq \frac{k+2}{2}$.
- $\text{lub}_\alpha \rho(\alpha) = \infty$, where the lub is over nonzero nonunits of $\mathbf{Z}[5i]$.