E. Dummit's Math 4527 ~ Number Theory 2, Spring 2025 ~ Homework 3, due Tue Jan 28th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Identify all pages containing each problem when submitting the assignment.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each value of D, use the super magic box to (i) find the continued fraction expansion for $\sqrt{D}$, (ii) find the fundamental unit in the ring $\mathbb{Z}[\sqrt{D}]$, (iii) determine whether the Pell's equation $x^2 - Dy^2 = -1$ has a solution and if so find the smallest one, and (iv) find the smallest two solutions to the Pell's equation $x^2 - Dy^2 = 1$:

   (a) $D = 19$. (b) $D = 22$. (c) $D = 130$. (d) $D = 61$.

---

2. Use the super magic box to factor each of the following integers:

   (a) 437. (b) 8137. (c) 15403.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

3. In class, we showed how to compute solutions to Pell's equation $x^2 - Dy^2 = \pm 1$ by taking powers of the fundamental solution $u = x_1 + y_1\sqrt{D}$ and then extracting coefficients of the resulting power. The goal of this problem is to give various formulas and recurrences for these coefficients. So suppose $u = x_1 + y_1\sqrt{D}$ is the fundamental solution to $x^2 - Dy^2 = \pm 1$ and let $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.

   (a) Show that $x_{n+1} = x_1 x_n + Dy_1 y_n$ and $y_{n+1} = y_1 x_n + x_1 y_n$.
   (b) Show that both sequences $\{x_n\}_{n\geq 1}$ and $\{y_n\}_{n\geq 1}$ satisfy the two-term recurrence relation $t_{n+2} = At_{n+1} + Bt_n$ where $A = 2x_1$ and $B = -(x_1^2 - Dy_1^2)$.
   (c) If $\overline{u} = x_1 - y_1\sqrt{D}$ is the conjugate of u, show that $x_n - y_n\sqrt{D} = \overline{u}^n$. Deduce that $x_n = \dfrac{u^n + \overline{u}^n}{2}$ and $y_n = \dfrac{u^n - \overline{u}^n}{2\sqrt{D}}$. [Hint: The conjugation map respects multiplication, just like complex conjugation does.]

   Remark: The reason that $\{x_n\}_{n\geq 1}$ and $\{y_n\}_{n\geq 1}$ satisfy the kind of two-term linear recurrences given in (b) is because x_{n+2}, x_{n+1}, y_{n+2}, and y_{n+1} are all linear combinations of x_n and y_n, and so the sets $\{x_{n+2}, x_{n+1}, x_n\}$ and $\{y_{n+2}, y_{n+1}, y_n\}$ are linearly dependent as functions. Furthermore, the general theory of linear recurrences says that the solutions to a recurrence of the form $t_{n+2} = At_{n+1} + Bt_n$ are given by $t_n = c\alpha^n + d\beta^n$ where α and β are the roots of the characteristic polynomial $t^2 - At - B$ and c, d are some constants. Part (b) shows that the characteristic polynomial for both recurrences is $t^2 - 2x_1 t + (x_1 - Dy_1^2)$, which factors as $(t - u)(t - \overline{u})$: this is why in (c) the results are of the form $x_n, y_n = cu^n + d\overline{u}^n$ for some constants c, d.

---

4. The goal of this problem is to prove that if p is a prime congruent to 1 modulo 4, then there is always a solution to the negative Pell equation $x^2 - py^2 = -1$. As we showed, there exists a minimal solution (x_1, y_1) to $x^2 - py^2 = 1$ where x, y are positive and minimal.

   (a) Show that x_1 is odd, y_1 is even, and that $\gcd(x_1 + 1, x_1 - 1) = 2$.
   (b) Show either that $x_1 - 1 = 2ps^2$, $x_1 + 1 = 2t^2$ or that $x_1 - 1 = 2s^2$ and $x_1 + 1 = 2pt^2$ for some positive integers s, t. [Hint: Use $x_1^2 - 1 = py^2$ and $\gcd(x_1 + 1, x_1 - 1) = 2$.]
   (c) With notation as in (b), show that if $x_1 - 1 = 2ps^2$ and $x_1 + 1 = 2t^2$ then $t^2 - ps^2 = 1$, contradicting the minimality of (x_1, y_1). Conclude in fact that there is an integer solution to $x^2 - py^2 = -1$.

---

5. The goal of this problem is to establish some cases in which the negative Pell equation $x^2 - Dy^2 = -1$ has no solutions.

   (a) Suppose that D is divisible by 4. Show that $x^2 - Dy^2 = -1$ has no solutions.

   (b) Suppose that p is an odd prime and that there is a solution to the congruence $x^2 \equiv -1 \pmod{p}$. Prove that $p \equiv 1 \pmod{4}$. [Hint: Explain why x has order 4 in the multiplicative group of nonzero residues modulo p, and then use Lagrange's theorem or Euler's theorem.]

   (c) Suppose that D is divisible by a prime that is congruent to 3 modulo 4. Show that $x^2 - Dy^2 = -1$ has no solutions.

   (d) By (a)-(c) above, if $x^2 - Dy^2 = -1$ has solutions, then D is a product of primes congruent to 1 modulo 4, possibly times 2. In fact, not all such integers do have a solution to the negative Pell equation: show specifically that $x^2 - 34y^2 = -1$ and $x^2 - 221y^2 = -1$ have no solutions.

---

6. The goal of this problem is to construct uncountably many transcendental numbers.

   (a) Prove that the real number $\alpha = \sum_{k=1}^{\infty} \frac{1}{(k!)^{k!}} = 1 + \frac{1}{2^2} + \frac{1}{6^6} + \frac{1}{24^{24}} + \cdots$ is transcendental.

   (b) Generalize (a) by showing that any number of the form $\beta = \sum_{k=1}^{\infty} \frac{(-1)^{s_k}}{(k!)^{k!}}$ is transcendental, for any choice of signs $(-1)^{s_k} = \pm 1$ on each term.

   (c) Show that all of the numbers in (b) are distinct and lie in $(-2, 2)$. Deduce that there are uncountably many transcendental numbers in the interval $(-2, 2)$. [Hint: For distinctness, suppose that two of the numbers in (b) are equal and have their first unequal signs in the dth term. Show that the tails of the series are too small to account for the difference.]

   (d) Conclude in fact that there are uncountably many transcendental numbers in any open interval (a, b) for any $a < b$.

---

7. [Challenge] It is a theorem of Hurwitz, mentioned in class, that if α is an arbitrary irrational number, then there exist infinitely many p/q with $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\,q^2}$. The goal of this problem is to prove that $\sqrt{5}$ cannot be replaced by any larger constant (i.e., that Hurwitz's theorem is sharp). So let $C > \sqrt{5}$.

   (a) Let $\varphi = \frac{1+\sqrt{5}}{2} = [1, 1, 1, 1, \ldots]$ be the golden ratio and suppose that $\left|\varphi - \frac{p}{q}\right| < \frac{1}{Cq^2}$. Show that $\frac{p}{q} = \frac{F_{n+1}}{F_n}$ for some positive integer n, where F_n is the nth Fibonacci number, defined by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for each $n \geq 1$.

   (b) Suppose $\alpha = [a_0, a_1, a_2, \ldots]$. Show that $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}$.

   (c) Show that $\left|\varphi - \frac{F_{n+1}}{F_n}\right| = \frac{1}{F_n^2(\varphi + F_{n-1}/F_n)}$ and that $\lim_{n\to\infty} [\varphi + F_{n-1}/F_n] = \sqrt{5}$.

   (d) Deduce that if $C > \sqrt{5}$, then there are only finitely many rational numbers p/q such that $\left|\varphi - \frac{p}{q}\right| < \frac{1}{Cq^2}$.
