Math 437/537 Problem set 1 (due 16/9/09)

Euclid's Algorithm

1. Find the gcd and lcm of 1728 and 496. Show a complete calculation by hand.

The Fibonacci sequence

2. Define numbers f_n by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 1$. Show that $f_n \leq 2^n$ for all n. Conclude that the formal power series $F(x) = \sum_{n=0}^{\infty} f_n x^n$ has a positive radius of convergence.

3. Show that $F(x) = \frac{x}{1-x-x^2}$ (at least in the domain of convergence). Using the formula $\frac{1}{1-\alpha x} = \sum_{n=0}^{\infty} \alpha^n x^n$ find a closed-form expression for f_n.

4. Show that $\frac{\varphi^n}{\sqrt{5}} - 1 < f_n < \frac{\varphi^n}{\sqrt{5}} + 1$ where φ is the larger root of $t^2 - t - 1 = 0$.

5. Show that Euclid's algorithm for finding $\gcd(a,b)$ using subtractions requires at most $\log_{\varphi}(\max\{a,b\})$ subtractions.

Divisibility

Only use results about divisibility for this section; do not invoke the notion of a prime.

6. (More gcd identities)
   (a) Let $a,b \in \mathbb{Z}$ be relatively prime. Show that any divisor c of ab can be uniquely written in the form $c = a'b'$ with $a|a'$, $b|b'$.
   (b) Show that $\gcd(a,bc) = \gcd(a,b) \cdot \gcd(a,c)$ for any $a,b,c \in \mathbb{Z}$ with b,c relatively prime.
   (c) Show that $\gcd(ab,c) = \gcd(\gcd(a,c), \gcd(b,c))$ for any $a,b,c \in \mathbb{Z}$.

7. Let $x,a,b \in \mathbb{Z}_{\geq 1}$.
   (a) Show that $\gcd\left(x^a - 1, x^b - 1\right) = x^{\gcd(a,b)} - 1$.
   (b) Find $\gcd\left(x^a + 1, x^b + 1\right)$.

Algebra

8. Let A be a finite abelian group. For $x \in A$ and $d \in \mathbb{Z}$ write $d \cdot x$ for the sum of d copies of x (or $-d$ copies of $(-x)$ if $d < 0$).
   (a) For an integer d show that $A[d] = \{x \in A \mid d \cdot x = 0\}$ is a subgroup.
   (b) Show that $\sum_{x \in A} x = \sum_{x \in A[2]} x$.

9. For a prime p show that $(p-1)! \equiv -1\,(p)$.

Using the Gaussian Integers

For a complex number $z = x + iy$ write $\bar{z}$ for its complex conjugate $x - iy$, and Nz for its *norm* $z\bar{z} = x^2 + y^2$. We will study the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

10. Show that $\mathbb{Z}[i]$ contains $0, 1 \in \mathbb{C}$and is closed under addition and multiplication, in other words that it is a subring of $\mathbb{C}$. Establish the *well-ordering principle of* $\mathbb{Z}[i]$: a non-empty subset $S \subset \mathbb{Z}[i]$ contains $a \in S$ so that $Na \leq Nb$ for all $b \in S$.

11. (Sums of two squares) Say that $A \in \mathbb{Z}$ is *the sum of two squares* if there exist $a, b \in \mathbb{Z}$ so that $a^2 + b^2 = A$, that is if $A \in \{Nz \mid z \in \mathbb{Z}[i]\}$.
    (a) Show that $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ for all $z_1, z_2 \in \mathbb{C}$. Conclude that the norm is multiplicative.
    (b) Let $A, B \in \mathbb{Z}$ be each a sum of two squares. Show that AB is a sum of two squares.

12. (Euclidean property)
    (a) Let $a, b \in \mathbb{C}$ with $Nb \geq Na > 0$ and $Nb > \frac{1}{2}$. Show that one of $\mathrm{Re}(ab)$, $\mathrm{Im}(ab)$ has magnitude at least $\frac{1}{2}|a|^2$.
    (b) Under the same assumptions as in part (a), show that there exists $\varepsilon \in \{\pm 1, \pm i\}$ such that $N(b - \varepsilon a) < Nb$.
    (c) Show that for every $a, b \in \mathbb{Z}[i]$ with $a \neq 0$ there exist $q, r \in \mathbb{Z}[i]$ so that $b = qa + r$ and $Nr < Na$.