UE Discrete Mathematics

Exercises for Dec 12, 2023

91–93) **Note: Do not refer to integer factorization in your proofs!**

91) Prove: If x and y are odd integers, then $2 \mid (x^2 + y^2)$ but $4 \nmid (x^2 + y^2)$.

92) Let a, b, c, d be integers. Prove:

a) If $a \mid b$ and $a \mid c$, then for all integers x, y we have $a \mid (xb + yc)$.

b) If $\gcd(a, b) = 1$ and $c \mid a$ and $d \mid b$, then $\gcd(c, d) = 1$.

c) If $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$

93) Prove: If $\gcd(a, b) = 1$ then $\gcd(a + b, a - b)$ is either 1 or 2.

94) Use the Euclidean algorithm to find two integers a and b such that $2863a + 1057b = 42$.

95) Use the Euclidean algorithm to find all greatest common divisors of $x^3 + 5x^2 + 7x + 3$ and $x^3 + x^2 - 5x + 3$ in $\mathbb{Q}[x]$.

96) Let $(F_n)_{n \geq 0}$ be the Fibonacci sequence, i.e. $F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}$. Prove $\gcd(F_{n+2}, F_n) = 1$.

97) Prove that there exist infinitely many prime numbers p which are solutions of the equation $p \equiv 3 \mod 4$.

Hint: Assume that there are only finitely many such primes, say $p_1, \dots, p_n$, and consider the number $4p_1p_2 \cdots p_n - 1$.

98) Prove that in a commutative ring with 1 for all elements a and b and all units x we always have $\gcd(a, b) = \gcd(ax, b)$.

99) Consider the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (addition and multiplication taken from $\mathbb{C}$) and determine a greatest common divisor of $19 + 5i$ and $16 - 6i$.

Hint: You may assume without proof that $\mathbb{Z}[i]$ with $n(a + bi) = a^2 + b^2$ is a Euklidean ring. Now find q, r in $u = qv + r$ by determining $\frac{u}{v}$ in $\mathbb{Z}[i]$ and rounding real and imaginary part.

100) Which of the following mappings is well-defined?

a) $f : \mathbb{Z}_m \to \mathbb{Z}_m, \overline{x} \mapsto \overline{x^2}$,

b) $g : \mathbb{Z}_m \to \mathbb{Z}_m, \overline{x} \mapsto \overline{2^x}$.