MIDTERM SOLUTIONS

1. Find all positive n such that 3 divides $2^n - 1$.

Solution. Since $2 \equiv -1 \mod 3$, then $2^n \equiv (-1)^n \mod 3$. If n is odd $(-1)^n = -1$ and $2^n - 1 \equiv 1 \mod 3$. If n is even $(-1)^n = 1$ and $2^n - 1 \equiv 0 \mod 3$. So n must be even.

2. Is 21 a unit in $\mathbb{Z}_{2000}$? If yes, find its inverse.

Solution. Yes, since $(21, 2000) = 1$. The invers is 381 by use of Euclidean algorithm. Indeed, $2000 = 21 \cdot 95 + 5$, $21 = 5 \cdot 4 + 1$. So $5 = 2000 - 21 \cdot 95$,

$$1 = 21 - 5 \cdot 4 = 21 - (2000 - 21 \cdot 95) \cdot 4 = 21 \cdot 381 - 2000 \cdot 4.$$

3. List all subrings in $\mathbb{Z}_{35}$ and explain why your list is complete.

Solution. The list: $\{0\}$, $\{0, 5, 10, 15, 20, 25, 30\}$, $\{0, 7, 14, 21, 28\}$, $\mathbb{Z}_{35}$.

To prove that all subrings are listed above let R be a subring of $\mathbb{Z}_{35}$ and $R \neq \{0\}$. If $a \in R$ then $na \in R$ for any $n \in \mathbb{Z}$. Hence if $c = an + 35k$ with $n, k \in \mathbb{Z}$, then $[c] \in R$. Therefore $(a, 35) \in R$. Pick up $a \neq 0$ and $a \in R$. Then $(a, n) = 1, 5$ or 7. If $(a, n) = 1$, then $1 \in R$ and hence $R = \mathbb{Z}_{35}$. If $(a, n) = 5$, then $R = \{0, 5, 10, 15, 20, 25, 30\}$. If $(a, n) = 7$, then $R = \{0, 7, 14, 21, 28\}$.

4. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not isomorphic to $\mathbb{Q}$. ($\mathbb{Q}$ denotes the field of rational numbers).

Solution. Note that $\mathbb{Q} \times \mathbb{Q}$ is not a filed since $(1, 0)$ is not a unit. Therefore $\mathbb{Q} \times \mathbb{Q}$ is not isomorphic to $\mathbb{Q}$, because $\mathbb{Q}$ is a field.

5. (a) Prove that $x^4 + x^3 + 1$ is irreducible in $\mathbb{Z}_2[x]$.

(b) Prove that $x^4 + x^3 + 1$ is irreducible in $\mathbb{Q}[x]$.

Solution. (a) First, we check that $x^4 + x^3 + 1$ does not have roots in $\mathbb{Z}_2[x]$ by substituting $x = 0, 1$. Next we have to show that $x^4 + x^3 + 1$ is not divisible by any irreducible quadratic polynomial in $\mathbb{Z}_2[x]$. A quadratic polynomial is irreducible if and only if it does not have roots. All quadratic polynomials are x^2, $x^2 + x$, $x^2 + 1$ and $x^2 + x + 1$. The only irreducible polynomial is $x^2 + x + 1$. But $x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 1) + x$ so $x^2 + x + 1$ does not divide $x^4 + x^3 + 1$.

(b) Follows from (a) by Theorem 4.24.

6. Consider the subring S of real numbers which can be written in the form $a + b\sqrt{5}$ for some integers a and b.

(a) Prove that $a + b\sqrt{5}$ is a unit in S if and only if $a^2 - 5b^2 = \pm 1$.

(b) Prove that S has infinitely many units. (Hint: $(\sqrt{5} - 2)^n$ is a unit for any integer n).

Solution. (a) If $a^2 - 5b^2 = 1$, then $(a + b\sqrt{5})^{-1} = a - b\sqrt{5}$. If $a^2 - 5b^2 = -1$, then $(a + b\sqrt{5})^{-1} = -a + b\sqrt{5}$. Hence $a^2 - 5b^2 = \pm 1$ implies that $a + b\sqrt{5}$ is a unit in S.

To prove the statement in the opposite direction, observe that if $(a+b\sqrt{5})(c+d\sqrt{5})=1$, then $(a-b\sqrt{5})(c-d\sqrt{5})=1$. Therefore $a+b\sqrt{5}$ is a unit in S if and only if $a-b\sqrt{5}$ is a unit in S. A product of two units is a unit, because $(u_1u_2)^{-1}=u_2^{-1}u_1^{-1}$. Therefore if $a+b\sqrt{5}$ is a unit, then $(a+b\sqrt{5})(a-b\sqrt{5})=a^2-5b^2$ is a unit in S. But $(a^2-5b^2)^{-1}\in S$ implies $(a^2-5b^2)^{-1}\in\mathbb{Z}$. Hence $a^2-5b^2=\pm 1$.

(b) Since $((\sqrt{5}-2)^n)^{-1}=(\sqrt{5}+2)^n$, we have $(\sqrt{5}-2)^n$ is a unit for any integer n. Next we claim that $(\sqrt{5}-2)^n=(\sqrt{5}-2)^m$ implies $m=n$. Indeed, $(\sqrt{5}-2)^n=(\sqrt{5}-2)^m$ implies $(\sqrt{5}-2)^{m-n}=1$, which in turn implies $m=n$, because $|\sqrt{5}-2|<1$. Therefore for each integer n we have a unit in S and all these units are distinct. Hence there are infinitely many units in S.