# HW #9 Solutions

§20 #4. Using Fermat's theorem, find the remainder of $3^{47}$ when it is divided by 23.

Fermat's theorem implies that $3^{22} \equiv 1 \pmod{23}$. Thus,

$$3^{47} \equiv (3^{22})^2(3^3) = 1^2 \cdot 3^3 \equiv 27 \equiv 4 \pmod{23}$$

Hence, the remainder will be 4.

14. Describe all solutions of the given congruence, as we did in Examples 20.14 and 20.15.

$$45x \equiv 15 \pmod{24}$$

Since $\gcd(45, 24) = 3$ and $3 \mid 15$, from Theorem 20.12 there are exactly 3 solutions in $\mathbb{Z}_{24}$. Dividing by 3, we obtain the congruence $15x \equiv 5 \pmod 8$. Since $15 \equiv 7 \pmod 8$ and $7 \cdot 7 \equiv 49 \equiv 1 \pmod 8$, $15^{-1} = 7$ in $\mathbb{Z}_8$. Hence, $x \equiv 15^{-1} \cdot 5 \equiv 7 \cdot 5 \equiv 35 \equiv 3 \pmod 8$. Thus, $x \equiv 3 \pmod 8$. This implies that either $x \equiv 3 \pmod{24}$, $x \equiv 11 \pmod{24}$, or $x \equiv 19 \pmod{24}$. Hence, all solutions to the congruence are the integers in the three residue classes $3 + 24\mathbb{Z}$, $11 + 24\mathbb{Z}$, and $19 + 24\mathbb{Z}$.

§21 #2. Describe the field $F$ of quotients of the integral subdomain $D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$ of $\mathbb{R}$.

Consider the quotient
$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})} = \frac{ac-2bd+(bc-ad)\sqrt{2}}{c^2-2d^2}$$
$$= \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}$$

Since $a, b, c, d \in \mathbb{Z}$, $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} \in \mathbb{Q}(\sqrt{2}) = \{q_1 + q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\}$

Hence, $F \subseteq \mathbb{Q}(\sqrt{2})$. With the appropriate choice of $a, b, c$, and $d$, we can also show that $\mathbb{Q}(\sqrt{2}) \subseteq F$. Hence, $F = \mathbb{Q}(\sqrt{2})$.

§22 #22. Find a polynomial of degree $>0$ in $\mathbb{Z}_4[x]$ that is a unit.

$2x+1$ has degree 1 and is a unit in $\mathbb{Z}_4[x]$ with $(2x+1)^{-1} = 2x+1$ since $(2x+1)(2x+1) = 4x^2+4x+1 = 1$ in $\mathbb{Z}_4[x]$.

24. Prove that if $D$ is an integral domain, then $D[x]$ is an integral domain.

Proof: From Theorem 22.2, we know that $D[x]$ is a commutative ring with unity 1. We need only show that $D[x]$ contains no zero divisors. We wish to show that if $a(x)b(x)=0$, then $a(x)=0$ or $b(x)=0$. Instead, we will show the contrapositive: If $a(x)\neq 0$ and $b(x)\neq 0$, then $a(x)b(x)\neq 0$. Let $a(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$ and $b(x)=b_mx^m+b_{m-1}x^{m-1}+\dots+b_1x+b_0$ where $a_n\neq 0$ and $b_m\neq 0$. Then the leading coefficient of $a(x)b(x)$ is $a_nb_m$. Since $a_n\neq 0$, $b_m\neq 0$, and $D$ has no zero divisors, $a_nb_m\neq 0$. Therefore, $a(x)b(x)\neq 0$. Thus, $D[x]$ is an integral domain. ∎

§23. #6. Find all generators of the cyclic multiplicative group of units of the given finite field.

$\mathbb{Z}_7$

Consider $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ (the cyclic multiplicative group of units)

We have that $\langle 1\rangle = \{1\}$

$\langle 2\rangle = \{2,4,1\}$

$\langle 3\rangle = \{3,2,6,4,5,1\} = \mathbb{Z}_7^*$

$\langle 4\rangle = \{4,2,1\}$

$\langle 5\rangle = \{5,4,6,2,3,1\} = \mathbb{Z}_7^*$

$\langle 6\rangle = \{6,1\}$

Hence $\mathbb{Z}_7^*$ has generators 3 and 5.

12. Is $x^3+2x+3$ an irreducible polynomial in $\mathbb{Z}_5[x]$? Why? Express it as a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

We have that 4 is a root of $x^3+2x+3$ in $\mathbb{Z}_5$ since $4^3+2(4)+3=75=0$ in $\mathbb{Z}_5$. Thus, $x^3+2x+3$ is reducible in $\mathbb{Z}_5[x]$. Moreover, $x-4=x+1$ is a factor of $x^3+2x+3$ in $\mathbb{Z}_5[x]$.

$$
\begin{array}{r|l}
 & x^2 - x + 3 \\
\hline
x+1 & x^3 + 0x^2 + 2x + 3 \\
 & -(x^3 + x^2) \\
\hline
 & -x^2 + 2x \\
 & -(-x^2 - x) \\
\hline
 & 3x + 3 \\
 & -(3x + 3) \\
\hline
 & 0
\end{array}
$$

$$x^3 + 2x + 3 = (x+1)(x^2 - x + 3) = (x+1)(x^2 + 4x + 3)$$

$$= (x+1)(x+1)(x+3) = (x+1)^2(x+3) \quad \text{in } \mathbb{Z}_5[x]$$