Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
HW #2 Solutions

Section 20:
2) 2 is a generator of $\mathbb{Z}_{11}^{\times}$ as its powers are: 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 which hit every non-zero element.

3) 3 is a generator of $\mathbb{Z}_{17}^{\times}$ as its powers are: 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1 which hit every non-zero element.

4) Since $3^{22} \equiv 1 \pmod{23}$, we have that $3^{47} \equiv 3^{22\cdot 2+3} \equiv 3^3 \equiv 4 \pmod{23}$.

6) We first compute 2^{17} mod 18 by successive squaring. In $\mathbb{Z}_{18}$ we have

$$\begin{aligned}
2^2 &= 4\\
2^4 &= (2^2)^2 = 4^2 = 16\\
2^8 &= (2^4)^2 = 16^2 = (-2)^2 = 4\\
2^{16} &= (2^8)^2 = 4^2 = 16
\end{aligned}$$

Thus $2^{17} \equiv 2^{16}\cdot 2 \equiv 16 \cdot 2 = 14 \pmod{18}$ and $2^{17} = 18k + 14$ for some k.

Then by Fermat's little theorem, we know $2^{18} \equiv 1 \pmod{19}$ and thus

$$2^{2^{17}} \equiv 2^{18k+14} \equiv 2^{14} \pmod{19}.$$

Again we successively square but this time in $\mathbb{Z}_{19}$:

$$\begin{aligned}
2^2 &= 4\\
2^4 &= (2^2)^2 = 4^2 = 16\\
2^8 &= (2^4)^2 = 16^2 = (-3)^2 = 9
\end{aligned}$$

Thus

$$2^{2^{17}} \equiv 2^{14} \equiv 2^8 \cdot 2^4 \cdot 2^2 \equiv 4 \cdot 16 \cdot 9 \equiv 4 \cdot (-3) \cdot 9 \equiv 4 \cdot (-27) \equiv 4 \cdot 11 \equiv 44 \equiv 6 \pmod{19}.$$

8) We have that $\varphi(p^2)$ is the number of integers between 1 and p^2 that are relatively prime to p^2. Since a number is relatively prime to p^2 iff it is not divisible by p, we just need to know how many of these p^2 numbers are not divisible by p. Since exactly p of them are divisible by p (e.g. $p \cdot 1, p \cdot 2, \cdots, p \cdot p$), we see that $p^2 - p$ are not multiples of p. Thus $\varphi(p^2) = p^2 - p$.

10). By Euler's theorem, $7^{\varphi(24)} = 7^8 \equiv 1 \pmod{24}$. Thus,

$$7^{1000} \equiv 7^{8\cdot 125} \equiv (7^8)^{125} \equiv 1^{125} \equiv 1 \pmod{24}.$$

23)

a. False. This is not true for any $a \equiv 0 \pmod p$.

b. True.

c. True.

d. False. $\varphi(1) = 1$

e. True.

f. True.

g. False.

h. True.

i. False. $0x \equiv 1 \pmod p$ has no solution.

j. True.

24) All units in $\mathbb{Z}_{12}$ have order dividing 2 and thus this group of size 4 is the Klein 4-group ($\mathbb{Z}_2 \times \mathbb{Z}_2$).

27) We have

$$\begin{aligned} x \equiv x^{-1} \pmod p &\implies x^2 \equiv 1 \pmod p \\ &\implies x^2 - 1 \equiv 0 \pmod p \\ &\implies (x-1)(x+1) \equiv 0 \pmod p \\ &\implies x - 1 \equiv 0 \pmod p \text{ or } x + 1 \equiv 0 \pmod p \\ &\implies x \equiv \pm 1 \pmod p. \end{aligned}$$

Here the penultimate implication follows because $\mathbb{Z}_p$ is a field and thus an integral domain.

Section 21:
1) The field of quotients of $\mathbb{Z}[i]$ is $\mathbb{Q}(i) = \{a + bi \ : \ a, b \in \mathbb{Q}\}$.

2) The field of quotients of $\mathbb{Z}[\sqrt{2}]$ is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$.

4)

a. True.

b. False. The field of quotients is unique and since it is $\mathbb{Q}$ it can't be $\mathbb{R}$ as $\mathbb{Q}$ and $\mathbb{R}$ are not isomorphic.

c. True.

d. False. The field of quotients is unique and since it is $\mathbb{R}$ it can't be $\mathbb{C}$ as $\mathbb{C}$ and $\mathbb{R}$ are not isomorphic.

e. True.

f. True (subjective question though!)

g. False. 0 is not a unit.

h. True.

i. True.

j. True.

5) Let $\mathbb{Z}[1/2] = \{a/b \ : \ b \text{ is a power of } 2\}$. This is a ring and we have that $\mathbb{Z} \subseteq \mathbb{Z}[1/2] \subseteq \mathbb{Q}$. However, the field of quotients of both $\mathbb{Z}$ and $\mathbb{Z}[1/2]$ are $\mathbb{Q}$.

8) We compute that

$$\overline{(-a,b)} + \overline{(a,b)} = \overline{((-a)b + ba, b^2)} = \overline{(0,b^2)} = \overline{(0,1)} = 0$$

and thus $\overline{(-a,b)}$ is the additive inverse of $\overline{(a,b)}$.

10) We have

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)} = \overline{(ca,db)} = \overline{(c,d)} \cdot \overline{(a,b)}$$

and thus multiplication is commutative.

<u>Section 21</u>:

2) We have

$$x + 1 + x + 1 = 2x + 2 = 0 \text{ in } \mathbb{Z}_2[x]$$

and

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1 \text{ in } \mathbb{Z}_2[x].$$

6) Such polynomials have the form $a + bx + cx^2$ where a, b, c are in $\mathbb{Z}_5$. Since there are 5 choices for each of a, b and c, there are $5^3 = 125$ such polynomials.

14) The roots are 0 and 4.

24) Let $f(x)$ and $g(x)$ be non-zero polynomials in $D[x]$. Write $f(x) = a_d x^d + a_{d-1}x^{d-1} + \dots$ and $g(x) = b_e x^e + b_{e-1}x^{e-1} + \dots$ where a_d and b_e are non-zero. Then the leading term of $f(x)g(x)$ is given by $a_d b_e x^{d+e}$ and we know that $a_d b_e$ is non-zero since D is an integral domain and both a_d and d_e are non-zero. Thus $f(x)g(x)$ is non-zero and $D[x]$ is an integral domain.