

p. 189

#2 mod 11 we have:

$$2^1=2, 2^2=4, 2^3=8, 2^4=5, 2^5=10, 2^6=9, 2^7=7, 2^8=3, 2^9=6, \\ 2^{10}=1$$

so 2 is a generator. Other generators are 8, 7, 6

3. 3, 5, 6, 7, 10, 11, 12 or 14 all generate $(\mathbb{Z}_{11})^*$ which is cyclic of order 10

4. $\phi(23) = 22$ so $3^{22} \equiv 1 \pmod{23}$ so

$$3^{47} \equiv 3^3 \equiv 4 \pmod{23}$$

5. $\phi(17) = 16$ so $37^{16} \equiv 1 \pmod{17}$

Thus $37^{49} \equiv 37^1 \equiv 2 \pmod{17}$

6. $\phi(18) = 6$ so $2^6 \equiv 1 \pmod{9}$ so $2^{17} \equiv 2^5 \pmod{9}$
 $= 32 \equiv 5 \pmod{9}$

$$2^{17} \equiv 0 \pmod{2}$$

Thus $2^{17} \equiv 5 \pmod{9}$
 $\equiv 0 \pmod{2}$ so $2^{17} \equiv 14 \pmod{18}$

Now $2^{18} \equiv 1 \pmod{19}$ so

$$2^{2^{17}} \equiv 2^{14} \pmod{19}$$

But $\phi(19) = 18$ so $2^{18} \equiv 1 \pmod{19}$

$$\begin{aligned} 2^{14} \cdot 2^4 &\equiv 1 \\ 2^{14} \cdot 16 &\equiv 1 \\ \text{so } 2^{14} &\equiv \boxed{6} \text{ since } 6 \cdot 16 = 96 \equiv 1 \pmod{19} \end{aligned}$$

8. #s $< p^2$ but not rel prime to p^2 are

$$p, 2p, 3p, \dots, (p-1)p$$

$$\text{so } \phi(p^2) = (p^2 - 1) - (p-1) \\ = \boxed{p^2 - p}$$

9. $\phi(pq) = (p-1)(q-1)$ done in class

10. $\phi(24) = 8$ so $7^8 \equiv 1 \pmod{24}$

$$\text{so } 7^{1000} = (7^8)^{125} \equiv \boxed{1 \pmod{24}}$$

23. a. F (mod pka)

b. T

c. T

d. F ($\phi(1) = 1$)

e. T

f. T

g. F

h. T

i. F

27. $x^2 - 1 = (x+1)(x-1)$. Since \mathbb{Z}_p is an integral domain

this can be zero unless $x-1=0$ or $x+1=0$

i.e. $x=1$ or $x=-1$ but $-1 \equiv p-1$

So $1, p-1$ are only elements satisfying $x \cdot x = 1$

28.

$$(p-1)! = (p-1)(p-2) \cdots \cdot 3 \cdot 2 \cdot 1$$

Now mod p everything^{is} is invertible

so those terms pair up w/ their inverses,
except $p-1$ and 1 , by #2?

$$\text{Thus } (p-1)! \equiv (p-1)(1) \equiv p-1 \equiv -1 \pmod{p}$$

p 196

#2 $\{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ done in class

12

a. Let $t \in T$. Then (t, t) is an identity

$$(t, t) \cdot (a, t') = (ta, tt')$$

$$\text{But } (a, t') = (ta, tt')$$

since $att' = t'ta$ (commut ring!)

b. Let $x \in T$. Notice $x \cdot 1 = (xt, t)$ is invertible

$$\text{namely } (xt, t)^{-1} = (t, xt)$$

$$(xt, t) \cdot (t, xt) = (xt^2, xt^2) \sim (t, t)$$

13. Suppose $a \neq 0$ is not a zero divisor. Let

$$T = \{a^n \mid n \in \mathbb{Z}^+\}$$

Then T satisfies the assumption of #12

so $Q(R, T)$ is a comm. ring w/ unity.

$$14. \quad R \times T = \left\{ \begin{array}{ccc} (0,1) & (0,1) & (0,3) \\ (0,1) & (1,1) & (1,3) \\ (0,1) & (2,1) & (2,3) \\ & (3,1) & (3,3) \end{array} \right.$$

$$(0,1) \sim (0,3)$$

$$\text{but } (1,1) \sim (3,3)$$

$$(2,1) \sim (2,3) \quad (\text{since } 6 \equiv 2)$$

$$(3,1) \sim (1,3) \quad (\text{since } 9 \equiv 1)$$

Thus there are 4 eq. classes.

$$15. \quad \text{This is } \approx \text{ to } \left\{ \frac{a}{n} \in \mathbb{Q} \mid \begin{array}{l} b = \text{a power of } 2 \\ a, n \in \mathbb{Z} \end{array} \right\}$$

16. Fractions $\frac{a}{n}$ with $3|a$ and b a power of 6

17. Solution in fract. Netno \sim is not an eq. relation

since checking transitive property needed w/ zero divisors