MODEL ANSWERS TO THE SIXTH HOMEWORK

1. §20: 2. We want to find an element of $\mathbb{Z}_{11}$ of order 10. We just use trial and error. The order of any element divides 10, so if the order is neither 2 nor 5 then the order must be 10.

$$2^2 = 4 \qquad \text{and} \qquad 2^5 = 2 \cdot 2^4 = 2 \cdot 16 = 2 \cdot 5 = 10 \mod 11.$$

Neither of these are 1, so 2 has order 10. Thus 2 generates the group of units of $\mathbb{Z}_{11}$.

6. 19 is prime and so by Fermat we know that

$$2^{18} = 1 \mod 19.$$

So we'd first like to compute the remainder when we divide 18 into 2^{17}. This is half of the remainder when you divide 9 into 2^{16}. Note that

$$\begin{aligned} \phi(9) &= 9 - 3 \\ &= 6. \end{aligned}$$

By Euler's Theorem

$$2^6 = 1 \mod 18.$$

Thus

$$\begin{aligned} 2^{16} &= 2^{2 \cdot 6 + 4} \\ &= (2^6)^2 2^4 \\ &= 2^4 \\ &= 16 \\ &= -2 \mod 18. \end{aligned}$$

If we multiply this by 2 we get $-4 = 14 \mod 18$. Thus

$$\begin{aligned} 2^{2^{17}} &= 2^{14} \\ &= (2^4)^3 2^2 \\ &= (-3)^3 2^2 \\ &= -27 \cdot 2^2 \\ &= -8 \cdot 2^2 \\ &= -16 \cdot 2 \\ &= 3 \cdot 2 \\ &= 6 \mod 19. \end{aligned}$$

So the answer is $2^{2^{17}} = 6 + 1 = 7 \mod 19$.

8. Consider the elements of $\mathbb{Z}_{p^2}$. There are p^2 numbers between 0 and $p^2 - 1$. a is coprime to p^2 if and only if a is not divisible by p. There are p multiples of p between 0 and $p^2 - 1$,

$$0 \qquad p \qquad 2p \qquad 3p \qquad \dots \qquad (p-1)p = p^2 - p.$$

So $p^2 - p$ elements of $\mathbb{Z}_{p^2}$ are coprime to p. Thus

$$\phi(p^2) = p^2 - p.$$

10.

$$\begin{aligned} \phi(24) &= \phi(3 \cdot 8) \\ &= \phi(3)\phi(8) \\ &= (3-1)(8-4) \\ &= 2 \cdot 4 \\ &= 8. \end{aligned}$$

Thus Euler's Theorem implies that

$$7^8 = 1 \mod 24.$$

Therefore

$$\begin{aligned} 7^{1000} &= 7^{2^3 \cdot 5^3} \\ &= (7^8)^{5^3} \\ &= 1 \mod 24. \end{aligned}$$

23. T: (b), (c), (d), (e), (f), (h), (j)
F: (a), (g), (i).

27. Suppose that $a \in \mathbb{Z}_p$ is its own inverse. Then

$$a \cdot a = 1,$$

so that a is a solution of the polynomial equation

$$x^2 - 1 = 0.$$

On the other hand we can factor this polynomial in $\mathbb{Z}_p$ in the usual way

$$x^2 - 1 = (x-1)(x+1),$$

so that

$$(a-1)(a+1) = 0.$$

Since $\mathbb{Z}_p$ is a field, we can cancel, unless $a - 1 = 0$ or $a + 1 = 0$. In this case $a = 1$ or $a = -1 = p - 1$. Conversely $a = 1$ and $a = p - 1$ are their own multiplicative inverses.

2. §21: 2. F is the set of all real numbers of the form

$$\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}.$$

4. T: (a), (c), (e), (f), (i), (j)
F: (b), (d), (g).
3. **Challenge Problems** §20: 28. Consider writing out the product:

$$(p-1)! = (p-1)(p-2)(p-3)\dots 1.$$

The numbers from 1 to $p-1$ consist of all the units of $\mathbb{Z}_p$. Every unit a has an inverse b and $ab = 1$. So if we pair all the units with their inverses in this product what is left is the product of all elements which are their own inverse. By 27 this consists of 1 and $p-1$. So

$$\begin{aligned}(p-1)! &= (p-1)(p-2)(p-3)\dots 1\\ &= (p-1)1\\ &= (p-1)\\ &= -1 \mod p.\end{aligned}$$

29. As suggested

$$m = 383838 = 37 \cdot 19 \cdot 13 \cdot 7 \cdot 3 \cdot 2.$$

is the prime factorisation of 383838. As $n^{37} - n$ is divisible by m if and only if it is divisible by each prime factor, it suffices to check that $n^{37} - n$ is divisible by $p = 2$, 3, 7, 13, 19 and 37, that is, the remainder is zero.
As $n^{37} - n = n(n^{36} - 1)$ if n is a multiple of p there is nothing to prove. Otherwise we may assume that n is coprime to p and it suffices to prove that

$$n^{36} = 1 \mod p.$$

By Fermat's Theorem we know that

$$n^{p-1} = 1 \mod p,$$

and so it is enough to check that $p-1$ divides 36. Note that $p-1$ is equal to 1, 2, 6, 12 and 36 all of which divide 36.
Thus $n^{37} - n$ is divisible by 383838.
30. The divisors of 36 are 1, 2, 3, 4, 6, 12, 18 and 36. If we add one to these numbers we get 2, 3, 4, 5, 7, 13, 19 and 37. Of these, 2, 3, 5, 7, 13, 19 and 37 are prime. Fermat's Theorem implies that if n is not a multiple of one of these primes p then $n^{36} - 1$ is divisible by p.
So p divides $n^{37} - n$. Thus the product

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 = 1919190$$

divides $n^{37} - n$.