PMATH 340 Number Theory, Solutions to the Exercises for Chapter 3

1: (a) Make a table of powers in $\mathbf{Z}_{21}$, showing the values of x^k for all $x \in \mathbf{Z}_{21}$ and all $1 \leq k \leq 7$.

Solution: Here is the table of powers modulo 21.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
x^2	0	1	4	9	16	4	15	7	1	18	16	16	18	1	7	15	4	16	9	4	1
x^3	0	1	8	6	1	20	6	7	8	15	13	8	6	13	14	15	1	20	15	13	20
x^4	0	1	16	18	4	16	15	7	1	9	4	4	9	1	7	15	16	4	18	16	1
x^5	0	1	11	12	16	17	6	7	8	18	19	2	3	13	14	15	4	5	9	10	20
x^6	0	1	1	15	1	1	15	7	1	15	1	1	15	1	7	15	1	1	15	1	1
x^7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

(b) Find the order of each element in U_{21}.

Solution: Using the table in part (a) we can list the orders:

x	1	2	4	5	8	10	11	13	16	17	19	20
$\lvert x\rvert$	1	6	3	6	2	6	6	2	3	6	6	2

(c) Solve $x^{100} = x$ in $\mathbf{Z}_{21}$.

Solution: In $\mathbf{Z}_{21}$ the table of powers repeats every 6 rows beginning with row 1, and $100 = 4$ mod 6, so $x^{100} = x^4$ for all $x \in \mathbf{Z}_{21}$, and from row 4 of the table of powers we have

$$x^{100} = x \iff x^4 = x \iff x = 0, 1, 4, 7, 9, 15, 16 \text{ or } 18\,.$$

2: (a) Find 7^{24}, 143^{962} and 1102^{1101} mod 1100.

Solution: Note that $1100 = 2^2 \cdot 5^2 \cdot 11$ so $\psi(1100) = \operatorname{lcm}(2, 20, 10) = 20$ and $k(1100) = 2$: the table of powers repeats every 20 rows beginning with row 2. Since $24 = 4$ mod 20 we have $7^{24} = 7^4 = 2401 = 201$ mod 1100. Since $962 = 2$ mod 20 we have $143^{962} = (143)^2 = 20449 = 649$ mod 1100. Since $1102 = 2$ mod 1100 and 1101=1=21 mod 20 we have $1102^{1101} = 2^{21} = 2097152 = 552$ mod 1100.

(b) Find 4210^{2142} mod 6300.

Solution: $6300 = 2^2 \cdot 3^2 \cdot 7 \cdot 5^2$ so $\psi(6300) = \operatorname{lcm}(2, 6, 6, 20) = 60$ and $k(6300) = 2$: the table of powers repeats every 60 rows beginning with row 2. Since 2142=42 mod 60 we have $4210^{2142} = 4210^{42}$ mod 6300. Note that 42=32+8+2, so $4210^{42} = 4210^{32} \cdot 4210^{8} \cdot 4210^{2}$. We make a list of powers of 4210 modulo 6300:

k	1	2	4	8	16	32	42
4210^k	4210	2200	1600	2200	1600	2200	4600

Thus $4210^{2142} = 4600$ mod 6300.

3: (a) Find $523^{470^{654}}$ mod 37.

Solution: Note that $523 = 5$ mod 37, $\psi(37) = 36$, 470=2 mod 36, $\psi(36) = \psi(2^2 \cdot 3^2) = \operatorname{lcm}(2, 6) = 6$, 654=0=6 mod 6 and $2^6 = 64 = 28$ mod 36, and so $523^{470^{654}} = 5^{2^6} = 5^{28} = 5^{16} \cdot 5^8 \cdot 5^4$ mod 37. We make a list of powers of 5 modulo 37:

k	1	2	4	8	16	28
5^k	5	25	33	16	34	7

Thus $523^{470^{654}} = 7$ mod 37.

(b) Find $60^{59^{58^{57^{\cdots 1}}}}$ mod 19

Solution: 60=3 mod 19, $\psi(19) = 18$, 59=5 mod 18, $\psi(18) = 6$, 58=4 mod 6, $\psi(6) = 2$ and 57=1 mod 2, so

$$60^{59^{58^{57^{\cdots 1}}}} = 3^{5^{4^{1}}} = 3^{13} = 3^8 \cdot 3^4 \cdot 3^1 = 6 \cdot 5 \cdot 3 = 90 = 14 \text{ mod } 19\,.$$

4: (a) Find the largest integer n such that $\psi(n)=12$.

Solution: We begin by finding $\phi(p^k)$ for all prime powers p^k for which $\phi(p^k)\leq 12$:

$$\begin{array}{llllll} \phi(2)=1 & \phi(3)=2 & \phi(5)=4 & \phi(7)=6 & \phi(11)=10 & \phi(13)=12 \\ \phi(4)=2 & \phi(9)=6 & & & & \\ \phi(8)=4 & & & & & \\ \phi(16)=8 & & & & & \end{array}$$

For each prime p we choose the largest value of $k\geq 0$ for which $\phi(p^k)\big|12$, then we multiply these prime powers together to get $n=8\cdot 9\cdot 5\cdot 7\cdot 13=32760$.

(b) Find every positive integer n such that $\phi(n)=60$.

Solution: We begin by finding $\phi(p^k)$ for all prime powers p^k for which $\phi(p^k)\leq 60$, and we list those for which $\phi(p^k)\big|60$:

$$\begin{array}{llllllll} \phi(2)=1 & \phi(3)=2 & \phi(5)=4 & \phi(7)=6 & \phi(11)=10 & \phi(13)=12 & \phi(31)=30 & \phi(61)=60 \\ \phi(4)=2 & \phi(9)=6 & \phi(25)=20 & & & & & \\ \phi(8)=4 & & & & & & & \end{array}$$

Note that the only four prime powers p^k on this list for which $\phi(p^k)$ is a multiple of 5 are $p^k=11$, 25, 31 and 61, so to get $\phi(n)=60$, one of these four prime powers must be a factor of n. Also note that 25 cannot be a factor of n since $60=\phi(25)\cdot 3$ and there is no prime power p^k with $\phi(p^k)=3$. Thus n must have a factor of 11, 31 or 61. This helps to list all the possible values for n:

$$n=61,\ 61\cdot 2=124,\ 31\cdot 3=93,\ 31\cdot 3\cdot 2=186,\ 31\cdot 4=124,\ 11\cdot 7=77,\ 11\cdot 7\cdot 2=154,\ 11\cdot 9=99,\text{ or } 11\cdot 9\cdot 2=198\,.$$

From smallest to largest, the possible values for n are 61, 77, 93, 99, 122, 124, 154, 186 and 198.

5: (a) U_{81} is cyclic and is generated by 2, so we have $U_{81}=\left\{1,2,2^2,2^3,\cdots,2^{53}\right\}$. Find the number of squares, the number of cubes, and the number of twelfth powers in U_{81}.

Solution: Recall that for an element a of order $|a|=n$ in a finite group G, we have $\langle a^k\rangle=\langle a^d\rangle$ where $d=\gcd(k,n)$ and $|a^k|=n/d$. In U_{81} we have $|2|=|U_{81}|=\phi(81)=54$. The set of squares in U_{81} is the set $Q_{81}=\langle 2^2\rangle=\{1,2^2,2^4,2^6,\cdots\}$, and so the number of squares in U_{81} is $|Q_{81}|=|2^2|=\frac{54}{\gcd(2,54)}=\frac{54}{2}=27$. The set of cubes in U_{81} is the set $\langle 2^3\rangle=\{1,2^3,2^6,2^9,\cdots\}$ so the number of cubes is $|2^3|=\frac{54}{\gcd(3,54)}=\frac{54}{3}=18$. The set of twelfth powers is $\langle 2^{12}\rangle$ and the number of twelfth powers is $\frac{54}{\gcd(12,54)}=\frac{54}{6}=9$. More generally, if $n=p^k$ where p is an odd prime, then the number of m^{th} powers in U_n is equal to $\frac{\phi(n)}{\gcd(m,\phi(n))}$.

(b) U_{128} is generated by -1 and 5 and we have $U_{128}=\left\{\pm 1,\pm 5,\pm 5^2,\cdots,\pm 5^{31}\right\}$. Find the number of squares, the number of cubes, and the number of twelfth powers in U_{128}.

Solution: In U_{128} we have $|5|=32$. The set of squares in U_{128} is the set $Q_{128}=\langle 5^2\rangle=\{1,5^2,5^4,5^6,\cdots\}$ so the number of squares is $|Q_2|=|5^2|=\frac{32}{\gcd(2,32)}=\frac{32}{2}=16$. The set of cubes is generated by -1 and 5 and is equal to $\{\pm 1,\pm 5^3,\pm 5^6,\pm 5^9,\cdots\}$ so the number of cubes is $2\cdot|5^3|=\frac{2\cdot 32}{\gcd(3,32)}=64$. The set of twelfth powers is $\langle 5^{12}\rangle=\{1,5^{12},5^{24},5^{36}=5^4,\cdots\}$ so the number of twelfth powers is $|5^{12}|=\frac{32}{\gcd(12,32)}=\frac{32}{4}=8$. More generally, if $n=2^k$ with $k\geq 3$, then the number of m^{th} roots in U_n is equal to $\frac{2^{k-2}}{\gcd(m,2^{k-2})}$ if m is even and $\frac{2^{k-1}}{\gcd(m,2^{k-2})}$ if m is odd.