# CSE230: Discrete Mathematics

Practice Sheet 5: **Number Theory**

| | |
|---|---|
| Q1 | Determine whether $4 \mid 7$ and whether $4 \mid 24$ |
| Q2 | What are the quotient and remainder when<br>a) 193 is divided by 7?<br>b) −42 is divided by 5?<br>c) 597 is divided by 23?<br>d) 30201 is divided by 33?<br>e) 0 is divided by 18?<br>f ) 3 is divided by 8? |
| Q3 | What are the possible remainders (according to the Division Algorithm) when an integer is<br>a) Divided by 4?<br>b) Divided by 9? |
| Q4 | For each of the following, find the quotient and remainder (guaranteed by the Division Algorithm)<br>a. When 17 is divided by 3.<br>b. When -17 is divided by 3.<br>c. When 73 is divided by 7.<br>d. When -73 is divided by 7.<br>e. When 436 is divided by 27.<br>f. When 539 is divided by 110. |
| Q5 | Today is Tuesday. Your uncle will come after 45 days. On which day (of the week) your uncle will be coming? |
| Q6 | Find the value of $(177 \textbf{ mod } 31 \cdot 270 \textbf{ mod } 31) \textbf{ mod } 31$ |
| Q7 | Show that if $a \mid b$ and $b \mid a$, where $a$ and $b$ are integers, then $a = b$ or $a = -b$. |
| Q8 | Prove or disprove that if $a \mid bc$, where $a$, $b$ and $c$ are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$. |
| Q9 | Prove that if $a$ is an integer that is not divisible by 3, then $(a + 1)(a + 2)$ is divisible by 3. |
| Q10 | Let $m$ be a positive integer. Show that $a \textbf{ mod } m = b \textbf{ mod } m$ if $a \equiv b \pmod{m}$. |
| Q11 | Considering $a$ and $b$ are integers, and<br>$a \equiv b + 7 \ (\textbf{mod } 19)$, show that $(a^2 - 11) \equiv (b^2 - 5b) \ (\textbf{mod } 19)$ |

| | |
|---|---|
| Q12 | If we consider $50 \equiv 23 \pmod 9$, then prove that $34 \equiv 16 \pmod 9$<br>[Hint: Use the Theorem 5] |
| Q13 | 28. Find $a$ **div** $m$ and $a$ **mod** $m$ when<br>a) $a = -991$, $m = 99$.<br>b) $a = -119$, $m = 101$.<br>c) $a = 10299$, $m = 999$.<br>d) $a = 12346$, $m = 101$ |
| Q14 | Find the integer $a$ such that<br>a) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$.<br>b) $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$.<br>c) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$.<br>d) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$. |
| Q15 | Use modular exponentiation to find:<br>i) 7^64 **mod** 645.<br>ii) 32^203 **mod** 99.<br>iii) 22^3219 **mod** 243. |
| Q16 | i) What is the octal and hexadecimal expansion of $(11011000110\ 01011)_2$.<br>ii) What is the hexadecimal expansion of $(125110)_{10}$.<br>iii)What is the decimal expansion of $(7716)_8$.<br>iv) What is the binary expansion of $(\text{BADDAD})_{16}$.<br>v) What is the octal expansion of $(12344321)_{10}$. |
| Q17 | Expand the decimal number $(506070)_{10}$ to the base $\boldsymbol{x}$, where $\boldsymbol{x} = ((10*2^2)^2 + 72)$ **mod** 23. |
| Q18 | If $(ab)_4$ is a base-4 integer and $(ba)_7$ is a base-7 integer, what is the largest possible value of $(a+b)_{10}$ and why? Find non-zero values for a and b such that $(ab)_4=(ba)_7$, or prove that there are none. |
| Q19 | Determine whether the integers in each of these sets are **pairwise relatively prime**:<br>i) 14, 17, 85.<br>ii) 21, 34, 55.<br>iii) 25, 41, 49, 64.<br>iv) 17, 18, 19, 23. |
| Q20 | Consider two positive integers 5271 and 48714. Calculate the Greatest Common Divisor for the integers using Euclidean Algorithm. Also show the Least Common Multiple. |
| Q21 | Find the greatest common divisor of the following pair of numbers using the **Euclidean Algorithm**: |

| | |
|---|---|
| | i) 11111, 111111.<br>ii) 1529, 14038.<br>iii) 750, 900.<br>iv) 414, 662. |
| Q22 | How many divisions are required to find gcd(21, 34) using the **Euclidean algorithm**? |
| Q23 | Find gcd(92928, 123552) and lcm(92928, 123552), and verify that gcd(92928, 123552) · lcm(92928, 123552) = 92928 · 123552 |
| Q24 | If the product of two integers is 2^7 · 3^8 · 5^2 · 7^11 and their greatest common divisor is 23345, what is their least common multiple? |
| Q25 | Determine whether the integers in each of these sets are pairwise relatively prime.<br>a) 11, 15, 19<br>b) 14, 15, 21<br>c) 12, 17, 31, 37<br>d) 7, 8, 9, 11 |
| Q26 | If $p$ is a prime number, $p > 3$, then show that $p^2 \equiv p^4 \equiv 1 \pmod 3$ |
| Q27 | Work out the GCD of 7105, 3185 and 2898 **only using the Euclidean Algorithm**.<br>Note that, $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ |
| Q28 | Given that, the square root of a number $\boldsymbol{n}$ when divided by 11 gives a remainder of 6 where $\mathbf{6 < \sqrt{n} < 28}$. Find the number $\boldsymbol{n}$. Then, using modular exponentiation, calculate: $\boldsymbol{n^{125} \; mod \; 27}$. |