Supplementary Exercises on Number Theory

Note: These exercises are meant to help you revise the material that you have learnt in class when preparing for the exam. Please note that when solutions are given below for the problems, they are at most sketch solutions and do not provide derivations of the answers. For assignments and exams you are expected to provide full derivations. See the posted solutions to assignments for examples of this.

1. How many nonzero elements does the set Z_n have?
2. Prove that "$a \bmod n = b \bmod n$" implies "$(a + c) \bmod n = (b + c) \bmod n$" for any integer c.
3. Prove that "$a \bmod n = b \bmod n$" implies "$ac \bmod n = bc \bmod n$" for any integer c.
4. Prove that "$a \bmod n = b \bmod n$" and "$c \bmod n = d \bmod n$" imply "$(a + c) \bmod n = (b + d) \bmod n$".
5. Prove that "$a \bmod n = b \bmod n$" and "$c \bmod n = d \bmod n$" imply "$ac \bmod n = bd \bmod n$".
6. Find the multiplicative inverse of a in Z_m for each of the following:
   (a) $a = 15$, $m = 127$
   (b) $a = 61$, $m = 124$
   (c) $a = 12$, $m = 111$
   (d) $a = 82$, $m = 97$
   (e) $a = 3$, $m = 100$
   (f) $a = 1001$, $m = 1234$
7. (a) Let a be a positive integer. Show that $gcd(a, a - 1) = 1$.
   (b) Use the result of part (a) to solve the (Diophantine) equation $a+b = ab$, i.e., to find positive integers a, b solving the equation.
8. Compute the results of the following statements:
   (a) $5 \cdot 8 \bmod 9$
   (b) $(451 \cdot 25 + 7 \cdot 8) \bmod 41$
   (c) $2^{30} \bmod 15$

9. Use Euclid's GCD algorithm to compute the greatest common divisor of the following pairs of numbers:

   (a) 54, 21

   (b) 693, 147

   (c) 82, 97

10. For all positive integers a and b, prove that $gcd(ka, kb) = k \cdot gcd(a, b)$ for all positive integer k.

11. Prove that if $d \mid x$ and $d \mid y$, then $d \mid (x - y)$ and $d \mid (x + y)$.

12. Find $gcd(1112, 1544)$ and express it in the form $1112x + 1544y$ for some integers x and y.

13. Show that for any integer n, exactly one of $n, n + 2, n + 4$ is divisible by 3. In particular, except for $3, 5, 7$, there are no triples of prime numbers occurring in the pattern $n, n + 2, n + 4$.

14. Let n be a nonnegative integer. Prove that n and n^5 have the same last digit. For example:

$$\begin{aligned} \underline{2}^5 &= 3\underline{2} \\ 7\underline{9}^5 &= 307705639\underline{9} \end{aligned}$$

15. Given that $k \bmod 4 = 2$, find $(7k + 17) \bmod 4$.

16. Given that $k \bmod 4 = 3$, find $(9k^{333} + 22) \bmod 4$.

17. Compute the value of $(7^{3(2k+1)}) \bmod 43$ where $k \in \mathbb{Z}^+$.

18. Using a Caesar cipher with a shift of 4 to the right,

   (a) What is the ciphertext of "HELLO"?

   (b) What is the plaintext of "XAS"?

19. Let x be in Z_{15}. If $x \bmod 3 = 1$ and $x \bmod 5 = 3$, what is x?

20. Let x be in Z_{91}. If $x \bmod 7 = 4$ and $x \bmod 13 = 7$, what is x?

Solutions/Hints

1. $n-1$

2.

$$\begin{aligned} a \bmod n = b \bmod n &\Rightarrow (a-b) \bmod n = 0 \\ &\Rightarrow ((a+c)-(b+c)) \bmod n = 0 \\ &\Rightarrow (a+c) \bmod n = (b+c) \bmod n \end{aligned}$$

3.

$$\begin{aligned} a \bmod n = b \bmod n &\Rightarrow (a-b) \bmod n = 0 \\ &\Rightarrow (a-b)c \bmod n = 0 \\ &\Rightarrow ac \bmod n = bc \bmod n \end{aligned}$$

4. Similar to above, we have $(a-b) \bmod n = 0$ and $(c-d) \bmod n = 0$, which imply $((a+c)-(b+d)) \bmod n = 0 \Rightarrow (a+c) \bmod n = (b+d) \bmod n$.

5. From above, we have $(ac-bc) \bmod n = 0$ and $(bc-bd) \bmod n = 0$, which imply $(ac-bc+bc-bd) \bmod n = 0 \Rightarrow ac \bmod n = bd \bmod n$.

6. (a) 17
   (b) 61
   (c) does not exist
   (d) 84
   (e) 67
   (f) 1091

7. (a) $gcd(a, a-1) = gcd(a-1, a-(a-1)) = gcd(a-1, 1) = 1$. Since a is positive, we have $gcd(a-1, 1) = 1$.
   (b) Since $a = b(a-1)$, $a-1$ is a common divisor of a and $a-1$. However, since $gcd(a, a-1) = 1$, the only common divisor of a and $a-1$ is 1, i.e., $a-1 = 1$ or $a = 2$. Substituting this into the Diophantine equation gives $2+b = 2b$, which implies that $b = 2$.

8. (a) 4
   (b) 15
   (c) 4

9. (a) 3
   (b) 21

(c) 1

10. HINT: Let $gcd(a, b) = c$. Then we can write $a = sc$ and $b = tc$ for some positive integers s and t such that $gcd(s, t) = 1$.

11. HINT: Let $x = sd$ and $y = td$ for some integers s and t.

12. $8 = 1112 \cdot 25 + 1544 \cdot (-18)$

13. HINT: Consider three cases: $n = 3m$, $n = 3m + 1$, $n = 3m + 2$

14. The correctness of RSA relies on the following fact: if p and q are distinct prime numbers, then

$$m^{1+k(p-1)(q-1)} \bmod pq = m \bmod pq$$

for all m and k. Setting $k = 1$, $p = 5$ and $q = 2$ proves the claim.

15. $(7k + 17) \bmod 4 = (3 \cdot 2 + 1) \bmod 4 = 3$

16. Since $k \bmod 4 = 3 = -1 \bmod 4$, $(9k^{333} + 22) \bmod 4 = (1 \cdot (-1)^{333} + 2) \bmod 4 = (-1 + 2) \bmod 4 = 1$.

17. Since

$$7^3 \bmod 43 = 49 \cdot 7 \bmod 43 = 6 \cdot 7 \bmod 43 = 42 \bmod 43 = (-1) \bmod 43,$$

we have

$$(7^{3(2k+1)}) \bmod 43 = (-1)^{2k+1} \bmod 43 = (-1) \bmod 43 = 42.$$

18. (a) LIPPS

    (b) TWO

19. 13

20. 46