TMA4140
DISCRETE MATHEMATICS
NTNU, H2022

Exercise Set 7

Exercise sets are to be handed in individually by each student using the OVSYS system. Each set will be graded (godkjent / ikke godkjent). To get an exercise set approved you are required to have solved correctly at least 70% (providing detailed arguments/computations).
To be admitted to the exam in December (15/12/), you must have at least 4+4 set out of the 12 assignments approved. At least 4 of the approved exercises sets must be from the first 6 sets, and at least 4 must be from the last 6 exercise sets.
You are asked to pay attention to the quality of presentation, in particular, the correctness of mathematical notation and formalism.

Exercise 1. *Let A be a set and let $\pi = \{A_1, \ldots, A_k\}$ a set partition of A. We know that for each element $a \in A$ there exists a unique index $1 \leq j \leq k$ such that a is in $A_j \in \pi$. We define the map $\psi : A \to \pi$ by $\psi(x) = A_j$ if $x \in A_j$. Show that ψ is surjective. Is it injective (justify your answer)?*

Solution. Since π is a partition, all the sets in question are non-empty. For any element A_j in the partition we have a $x \in A_j$, and ψ maps this to A_j, so A_j is in the image. The entire codomain is in the image, so the function in surjective.

We do not have enough information to conclude whether the function is injective or not. If $k = 1$ and $A_1 = A = a$, then both A and the partition have a single element, so the function is clearly injective. If $k = 1$ and $A_1 = A = a, b$ then the domain has two elements while the codomain has one, so we do not get injectivity.

Exercise 2. *Consider the set* $[6] = \{1, 2, 3, 4, 5, 6\}$. *Let R be a relation defined on* $[6]$ *by:*

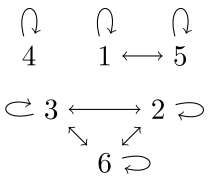
$$R = \{(1,1),(1,5),(2,2),(2,3),(2,6),(3,2),(3,3),(3,6),(4,4),(5,1),(5,5),(6,2),(6,3),(6,6)\}$$

i) *Verify that R determines an the equivalence relation on* $[6]$.
ii) *Draw the directed graph representing the relation R.*
iii) *Determine the set partition of* $[6]$ *induced by the relation R.*

Solution.

i) Since every pair (i, i) for $i \in [6]$ is in R it is reflexive. Symmetry can also be checked by simple inspection. For every pair (i, j) we can also find (j, i). Transitivity can be seen by taking every pair of pairs $((i, j), (k, l))$ and checking that if $j = k$ then (i, l) is in the R and if $i = l$ then (k, j) is in R. After checking this we conclude that since R is reflexive, symmetric and transitive it is an equivalence relation.

Date: October 4, 2022.

ii) 

iii) $\{\{1,5\},\{2,3,6\},\{4\}\}$

Exercise 3. *Of the following three systems of linear equations one has one solution, one has no solutions, and one has many solutions (modulo the product of the two moduli). Determine which one is which and explain why.*

i)

$$\begin{aligned} x &\equiv 7 \pmod{12} \\ x &\equiv 2 \pmod{9} \end{aligned}$$

ii)

$$\begin{aligned} x &\equiv 7 \pmod{12} \\ x &\equiv 3 \pmod{16} \end{aligned}$$

iii)

$$\begin{aligned} x &\equiv 3 \pmod{16} \\ x &\equiv 2 \pmod{9} \end{aligned}$$

Solution.

i) This system has no solutions since the right hand side modulus $\gcd(12,9)=3$ are different for the two equations.

ii) This system has many solutions since the right hand side modulus $\gcd(12,16)=4$ is equal for the two equations.

iii) This system has one solution since the moduli are relatively prime.

Exercise 4. *For the following four systems of linear equations, find all solutions (modulo the product of the moduli in the system).*

i)

$$\begin{aligned} x &\equiv 3 \pmod{19} \\ x &\equiv 1 \pmod{17} \end{aligned}$$

ii)

$$\begin{aligned} x &\equiv 32 \pmod{121} \\ x &\equiv 49 \pmod{81} \end{aligned}$$

iii)

$$\begin{aligned} x &\equiv 7 \pmod{11} \\ x &\equiv 2 \pmod{17} \\ x &\equiv 11 \pmod{15} \end{aligned}$$

iv)

$$x \equiv 8 \pmod{35}$$
$$x \equiv 29 \pmod{49}$$

Solution.

i) $17^{-1} \mod (19) = 9$, $19^{-1} \mod (17) = 9$, $x \equiv 1 \cdot 19 \cdot 9 + 3 \cdot 17 \cdot 9 \equiv 307 \pmod{323}$

ii) $81^{-1} \mod (121) = 3$, $121^{-1} \mod (81) = 79$, $x \equiv 32{\cdot}81{\cdot}3{+}49{\cdot}121{\cdot}79 \equiv 5719 \pmod{121{\cdot}81}$

iii) Starting by solving the first two equations. $11^{-1} \mod (17) = 14$, $17^{-1} \mod (11) = 2$, $x \equiv 7 \cdot 17 \cdot 2 + 2 \cdot 11 \cdot 14 \equiv 172 \pmod{11 \cdot 17}$ Putting this equation together with the last equation. $15^{-1} \mod (187) = 25$, $187^{-1} \mod 15 = 13$, $x \equiv 172 \cdot 15 \cdot 25 + 11 \cdot 187 \cdot 13 \equiv 1481 \pmod{2805}$

iv) $\gcd(35, 49) = 7$ By taking the right side of the first equation modulus 7 and dividing the modulus by 7 we get an equivalent system of equations;

$$x \equiv 3 \pmod{5}$$
$$x \equiv 29 \pmod{49}$$

Now the moduli are relatively prime, so we can continue as usual. $5^{-1} \mod (49) = 10$, $49^{-}1 \mod (5) = 4$. $x \equiv 3 \cdot 49 \cdot 4 + 29 \cdot 5 \cdot 10 \equiv 78 \pmod{245}$. If we want the solutions mod $(35 \cdot 49)$ instead, we get $x \equiv 78 + 245n \pmod{1715}$ for $n \in \{0, 1, 2, 3, 4, 5, 6\}$.

Exercise 5. *Calculate the following values of Euler's phi function.*

i) $\varphi(11)$
ii) $\varphi(125)$
iii) $\varphi(91)$
iv) $\varphi(72)$
v) $\varphi(455)$

Solution.

i) $\varphi(11) = 11 - 1 = 10$
ii) $\varphi(125) = \varphi(5^3) = 5^2(5 - 1) = 100$
iii) $\varphi(91) = \varphi(7 \cdot 13) = \varphi(7) \cdot \varphi(13) = (7 - 1)(13 - 1) = 72$
iv) $\varphi(72) = \varphi(2^3 \cdot 3^2) = 2^2(2 - 1) \cdot 3(3 - 1) = 24$
v) $\varphi(455) = \varphi(5 \cdot 7 \cdot 13) = (5 - 1)(7 - 1)(13 - 1) = 288$

Exercise 6. *Use Euler's Theorem to compute the following modular inverses.*

i) $7^{-1} \pmod{10}$
ii) $11^{-1} \pmod{45}$
iii) $13^{-1} \pmod{82}$
iv) $49^{-1} \pmod{100}$
v) $42^{-1} \pmod{121}$

Solution.

i) $7^{-1} \equiv 7^{\varphi(10)-1} = 7^3 \equiv 3 \pmod{10}$
ii) $11^{-1} \equiv 11^{\varphi(45)-1} = 11^{23} \equiv 41 \pmod{45}$

iii) $13^{-1} \equiv 13^{\varphi(82)-1} = 13^{39} \equiv 19 \pmod{82}$

iv) $49^{-1} \equiv 49^{\varphi(100)-1} = 49^39 \equiv 49 \pmod{100}$

v) $42^{-1} \equiv 42^{\varphi(121)-1} = 42^109 \equiv 49 \pmod{121}$

Exercise 7. *In the last exercise set you used the extended euclidean algorithm to compute modular inverses. In this exercise set you used Euler's Theorem. Comment on the benefits and/or drawbacks of using one method over the other.*

Solution. In order to use Euler's Theorem we have to know the factorization of the modulus.

Exercise 8. *Use Euler's Theorem to compute the following modular exponentiations.*

i) $13^{71924} \pmod{73}$

ii) $92^{61281} \pmod{323}$

iii) $100^{1012} \pmod{111}$

iv) $19^{314159265} \pmod{125}$

Solution.

i) $13^{71924} \equiv 13^{71924 \mod (\varphi(73))} = 13^{71924 \mod (72)} = 13^{68} \equiv 69 \pmod{73}$

ii) $92^{61281} \equiv 92^{61281 \mod (\varphi(323))} = 92^{61281 \mod (288)} = 92^{225} \equiv 58 \pmod{323}$

iii) $100^{1012} \equiv 100^{1012 \mod (\varphi(111))} = 100^{1012 \mod (72)} = 100^{4} \equiv 100 \pmod{111}$

iv) $19^{314159265} \equiv 19^{314159265 \mod (\varphi(125))} = 19^{314159265 \mod (100)} = 19^65 \equiv 49 \pmod{125}$

Exercise 9. *For the following pairs of primes p, q and encryption exponents e, generate the decryption exponent for the RSA cryptosystem and encrypt the message m.*

i) $p = 11$, $q = 19$, $e = 41$, $m = 42$

ii) $p = 13$, $q = 23$, $e = 29$, $m = 42$

iii) $p = 29$, $q = 37$, $e = 47$, $m = 42$

Solution.

i) $\varphi(11 \cdot 19) = 180$, $d = 41^{-1} \mod (180) = 101$, $c = m^e \mod (11 \cdot 19) = 207$

ii) $\varphi(13 \cdot 23) = 264$, $d = 29^{-1} \mod (264) = 173$, $c = 61$

iii) $\varphi(29 \cdot 37) = 1008$, $d = 47^{-1} \mod (1008) = 815$, $c = 557$

Exercise 10. *Factor n and use the factorization to decrypt the ciphertext c that has been encrypted using encryption exponent e.*

i) $n = 3337$, $e = 1111$, $c = 2903$

ii) $n = 1891$, $e = 1001$, $c = 1791$

iii) $n = 2581$, $e = 1011$, $c = 2545$

Solution.

i) $n = 47 \cdot 71$, $d = e^{-1} \mod (\varphi(n)) = 1111^{-1} \mod (\varphi(3337)) = 1111^{-1} \mod (3220) = 171$, $m = c^d \mod (n) = 42$

ii) $n = 31 \cdot 61$, $d = 1001^{-1} \mod (30 \cdot 60) = 401$, $m = 1791^{401} \mod (1891) = 42$

iii) $n = 29 \cdot 89$, $d = 1011^{-1} \mod (28 \cdot 88) = 1979$, $m = 2545^{1979} \mod (2581) = 42$