BM20A9200 Mathematics A – Exercise set 10

To be done by 20.–24.11.2023

Text in blue or red is not part of the problem or its solution. It's there as extra information to help you learn.

Exercise 1. Let $x \equiv 9 \pmod{24}$. Find all $y \in \mathbb{Z}$ such that $7x + 4 \equiv y \pmod{24}$.

Exercise 2. For each x and m below, find $y \in \{0, 1, 2, \dots, m-1\}$ such that $x \equiv y \pmod{m}$.

a) $x = 512 + 100 \cdot 33$ and $m = 99$,

b) $x = 12345678910$ and $m = 9$,

c) $x = 73 \cdot 56^4$ and $m = 50$,

d) $23x \equiv 1 \pmod{m}$ and $m = 25$.

Exercise 3. What is the remainder when

$$1! + 2! + 3! + 4! + 5! + 6! + \cdots + 2023!$$

is divided by 21?

Exercise 4. Prove that $2 \cdot 13^n + 7 \cdot 4^n$ is always divisible by 9 for any $n \in \mathbb{Z}_+$. If you don't immediately know how to do this, do your first try on scrap paper, and once you solve it, write the final solution in your main homework notebook

The following two exercises are encouraged to be done with Python! The function `pow(x,e,m)` calculates $x^e \bmod m$ efficiently.

Exercise 5. RSA encryption. Let $p = 109$ and $q = 131$ be two prime numbers.

a) (secret key holder) Compute the first half of the public key n, the secret ϕ and confirm that $e = 2^{12} + 1 = 4097$ is a suitable[1] second half of the public key (meaning: show that $\gcd(\phi, e) = 1$).

b) (message sender) Encrypt the message $M =$ `9876` using the public key consisting of n and e.

Exercise 6. RSA decryption. Let $p = 353$ and $q = 557$ be two prime numbers known only to the secret key holder (you). Let $n = p \cdot q = 196621$ be the first half of the encryption key and $e = 65537$ be the second half.

a) (secret key holder) Using your knowledge of p and q, compute a decryption key d corresponding to the encryption key (n, e).

b) (secret key holder) Using the key from b), decrypt the encrypted message $C =$ `156608` that was sent with the public key $(n, e) = (196621, 65537)$.

---

[1] Ideally it would take long to deduce ϕ from the knowledge of n and e. Common practice is to first select $e = 2^{16} + 1 = 65537$ or $e = 3$ and <u>only then</u> select p, q such that $n > e$ and $\gcd(\phi, e) = 1$.