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 $7x + 4 \equiv y \pmod{24}$.

Solution. Let's use the calculation rules for congruences:

$$\begin{aligned} x &\equiv 9 \pmod{24} && \| \cdot 7 \\ 7x &\equiv 63 \pmod{24} && \| 63 = 2 \cdot 24 + 15 \\ 7x &\equiv 15 \pmod{24} && \| + 4 \\ 7x + 4 &\equiv 19 \pmod{24}. \end{aligned}$$

Hence all numbers of the form $y = 24k + 19$ with $k \in \mathbb{Z}$ are the solutions to the problem.

Exercise 2. For each x and m below, find $y \in \{0, 1, 2, \ldots, m-1\}$ 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 $m = 25$.

Solution.

a) We have $512 = 5 \cdot 99 + 17$ so $512 \equiv 17 \pmod{99}$. Also $100 \equiv 1 \pmod{99}$, so $x \equiv 17 + 1 \cdot 33 \equiv 50 \pmod{99}$.

b) To find the remainder modulo 9 we can simpy calculate the reduced sum of digits.

$$\begin{aligned} x &\equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 1 + 0 \pmod{9} \\ &\equiv (4 + 5) + (3 + 6) + (2 + 7) + (1 + 8) + 9 + 1 + 0 \pmod{9} \\ &\equiv 1 \pmod{9} \end{aligned}$$

c) We have $73 \equiv 23 \pmod{50}$ and $56 \equiv 6 \pmod{50}$. The latter implies $56^4 \equiv 6^4 \equiv 1296 \equiv 46 \pmod{50}$. Hence $x \equiv 23 \cdot 46 \equiv 1058 \equiv 8 \pmod{50}$.

d) One solution is to write the congruence $23x \equiv 1 \pmod{25}$ as $23x = 1 + 25k$, where $x, k \in \mathbb{Z}$. Let's find one solutions to this using the Euclidean algorihtm:

$$\begin{aligned} 25 &= 1 \cdot 23 + 2 \\ 23 &= 11 \cdot 2 + 1 \end{aligned}$$

and reversing, we get $1 = 23 - 11 \cdot 2 = 23 - 11 \cdot (25 - 23) = 12 \cdot 23 - 11 \cdot 25$. Rewriting, we have $23 \cdot 12 = 1 + 25 \cdot (-11)$, so one solution is $x = 12$ and $k = -11$. The formula for all solutions gives $x = 12 + 25l$, $l \in \mathbb{Z}$. In other words, $x \equiv 12 \pmod{25}$.

Exercise 3. What is the remainder when

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

is divided by 21?

Solution. The remainder when dividing by 21 is the smallest non-negative integer r which is congruent to the original number modulo 21. We have:

$$\begin{aligned}
1! &\equiv 1 \pmod{21} \\
2! &\equiv 2 \pmod{21} \\
3! &\equiv 6 \pmod{21} \\
4! &\equiv 24 \equiv 3 \pmod{21} \\
5! &\equiv 5 \cdot 4! \equiv 5 \cdot 3 \equiv 15 \pmod{21} \\
6! &\equiv 6 \cdot 5! \equiv 6 \cdot 15 \equiv 90 \equiv 6 \pmod{21} \\
7! &\equiv 7 \cdot 6 \cdot 5! \equiv 21 \cdot 2 \cdot 5! \equiv 0 \cdot 2 \cdot 5! \equiv 0 \pmod{21}
\end{aligned}$$

because $21 \equiv 0 \pmod{21}$. All other terms have $7!$ as their factor, so they are all $\equiv 0 \pmod{21}$. Hence

$$\begin{aligned}
&1! + 2! + 3! + 4! + 5! + 6! + \cdots + 2023! \equiv 1! + 2! + 3! + 4! + 5! + 6! \\
&\equiv 1 + 2 + 6 + 3 + 15 + 6 \equiv 33 \equiv 12 \pmod{21}.
\end{aligned}$$

Hence the remainder is 12.

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

Solution.

Proof. Let's calculate everything modulo 9 and show that the value 0 modulo 9. This would imply that $2 \cdot 13^n + 7 \cdot 4^n = 0 + 9m$ for some $m \in \mathbb{Z}$, ergo that it's divisible by 9.

Firstly, we have $13 \equiv 4 \pmod{9}$. This implies that $13^n \equiv 4^n \pmod{9}$, and so

$$2 \cdot 13^n + 7 \cdot 4^n \equiv 2 \cdot 4^n + 7 \cdot 4^n \equiv 9 \cdot 4^n \equiv 0 \pmod{9}.$$

Being congruent to 0 modulo 9 means that the remainder is 0 when divided by 9. Hence $9 | 2 \cdot 13^n + 7 \cdot 4^n$ for all $n \in \mathbb{Z}_+$. □

This can also be shown by induction:

Proof. **Base case:** When $n = 1$ we have $2 \cdot 13^n + 7 \cdot 4^n = 2 \cdot 13 + 7 \cdot 4 = 26 + 28 = 54 = 9 \cdot 6$, so it is divisible by 9.

Induction step: Let's make the induction hypothesis: Assume that $9 \mid 2 \cdot 13^k + 7 \cdot 4^k$ for some $k \in \mathbb{Z}_+$. This means that $2 \cdot 13^k + 7 \cdot 4^k = 9m$ for some $m \in \mathbb{Z}$. Then, let's show that 9 divides $2 \cdot 13^{k+1} + 7 \cdot 4^{k+1}$. We have

$$\begin{aligned} 2 \cdot 13^{k+1} + 7 \cdot 4^{k+1} &= 2 \cdot 13^{k+1} + 4 \cdot 7 \cdot 4^k = 2 \cdot 13^{k+1} + 4 \cdot (9m - 2 \cdot 13^k) \\ &= 2 \cdot 13 \cdot 13^k + 36m - 8 \cdot 13^k = (26 - 8) \cdot 13^k + 36m = 18 \cdot 13^k + 36m \\ &= 9(2 \cdot 13^k + 4m). \end{aligned}$$

Hence under the induction assumption for $n = k$ we see that $9 \mid 2 \cdot 13^{k+1} + 7 \cdot 4^{k+1}$. The induction step is complete. □

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

Solution.

a) $n = pq = 109 \cdot 131 = 14279$ and $\phi = (p-1)(q-1) = 14040$. Then we just need to show that $\gcd(14040, 4097) = 1$. Let's calculate it:

$$\begin{aligned} 14040 &= 3 \cdot 4097 + 1749 \\ 4097 &= 2 \cdot 1749 + 599 \\ 1749 &= 2 \cdot 599 + 551 \\ 599 &= 1 \cdot 551 + 48 \\ 551 &= 11 \cdot 48 + 23 \\ 48 &= 2 \cdot 23 + 2 \\ 23 &= 11 \cdot 2 + 1 \end{aligned}$$

hence $\gcd(\phi, e) = 1$. In conclusion, $e = 4097$ is suitable.

b) To encrypt a message M with the public key (n, e), all we need to do is to calculate M^e mod n. In other words we must calculate 9876^{4097} mod 14279. As suggested, let's use python:

```
>>> pow(9876,4097,14279)
13512
```

[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 only then select p, q such that $n > e$ and $\gcd(\phi, e) = 1$.

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 $(n, e) = (196621, 65537)$.

Solution.

a) We need to find d such that $ed \equiv 1 \pmod{\phi}$ where $\phi = (p-1)(q-1) = 352 \cdot 556 = 195712$. We have $ed \equiv 1 \pmod{\phi}$ if and only if $\phi \mid (ed - 1)$. In other words, if and only if there is $k \in \mathbb{Z}$ such that

$$ed - 1 = k\phi.$$

This is equivalent to $ed - k\phi = 1$,

$$65537d - 195712k = 1.$$

Let's solve this using the Euclidean algorithm:

$$\begin{aligned} 195712 &= 2 \cdot 65537 + 64638 \\ 65537 &= 1 \cdot 64638 + 899 \\ 64638 &= 71 \cdot 899 + 809 \\ 899 &= 1 \cdot 809 + 90 \\ 809 &= 8 \cdot 90 + 89 \\ 90 &= 1 \cdot 89 + 1. \end{aligned}$$

From this let's solve for d and k by substituting the remainders from the above equations. We get

$$\begin{aligned} 1 &= 90 - 89 \\ &= 90 - (809 - 8 \cdot 90) = -809 + 9 \cdot 90 \\ &= -809 + 9 \cdot (899 - 809) = 9 \cdot 899 - 10 \cdot 809 \\ &= 9 \cdot 899 - 10 \cdot (64638 - 71 \cdot 899) = -10 \cdot 64638 + 719 \cdot 899 \\ &= -10 \cdot 64638 + 719 \cdot (65537 - 64638) = 719 \cdot 65537 - 729 \cdot 64638 \\ &= 719 \cdot 65537 - 729 \cdot (195712 - 2 \cdot 65537) = -729 \cdot 195712 + 2177 \cdot 65537 \end{aligned}$$

so we see that $65537 \cdot 2177 - 195712 \cdot 729 = 1$. Our candidate for d is the coefficient of $e = 65537$, so 2177. This number is non-negative and less than $\phi = 195712$, so it is suitable:

$$d = 2177.$$

b) If M is the original message and C the encrypted one, we have $C = M^e \bmod n$. To solve for M we have

$$M = C^d \bmod n = 156608^{2177} \bmod 196621.$$

To calculate that efficiently let's use Python's `pow`-function:

```
>>> pow(156608,2177,196621)
31337
```

Hence the secret message was 31337.