BM20A9200 Mathematics A – Exercise set 9

To be done by 13.–17.11.2023

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. Prove the following for all positive integers n:

a) if n is odd then $8 \mid n^2 - 1$,

b) if $3 \nmid n$ and n is odd then $24 \mid n^2 - 1$. **Hint:** $24 = 3 \cdot 8$ and $\gcd(3, 8) = 1$.

Solution.

a) Factor $n^2 - 1 = (n-1)(n+1)$. If n is odd then $n-1$ and $n+1$ are both even. Every second even number is divisible by 4 and since these are two consequtive even numbers one of them is divisible by 4 and the other by 2. Hence their product is divisible by 8.

b) From a) we know that $8 \mid n^2 - 1$. Since $24 = 3 \cdot 8$ and $\gcd(3, 8) = 1$ it's enough to show that $3 \mid n^2 - 1$. Every number has some integer m such that it can be written as $3m$, $3m + 1$ or $3m + 2$. Because $3 \nmid n$ we have $n = 3m + 1$ or $n = 3m + 2$. Then $n^2 = 9m^2 + 6m + 1$ or $n^2 = 9m^2 + 12m + 4$ which imply $n^2 - 1 = 3(3m^2 + 2m)$ or $n^2 - 1 = 3(3m^2 + 4m + 1)$. In both cases there is a factor of 3. Hence $3 \mid n^2 - 1$.

Exercise 2. Find some integer solution (where possible):

a) $3x - 5y = 7$

b) $21x - 35y = 24$

c) $97x + 127y = 1$

Solution. The equation $ax + by = c$ has an integer solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$. In that case a pair of solutions is found using the Euclidean algorithm for calculating $\gcd(a, c)$. For small numbers we can just use common sense.

a) Since 3 and 5 are prime numbers we have $\gcd(3, 5) = 1$ and 7 is its multiple. We have $1 = 6 - 5 = 3 \cdot 2 - 5 \cdot 1$, so multiplying by 7 gives the solution

$$7 = 3 \cdot 14 - 5 \cdot 7.$$

b) We have $21 = 3 \cdot 7$ and $35 = 5 \cdot 7$, so $\gcd(21, 35) = 7$. However $24/7 = 3.42\ldots \notin \mathbb{Z}$ meaning that 7 does not divide 24. For any integers x and y, the left-hand side is always a multiple of 7 but the righ-hand side not. Hence the equation has no integer solutions.

c) It is not easy to see the factors of 97 and 127. Let's use Euclidean algorithm:

$$\begin{aligned}
127 &= 1 \cdot 97 + 30 \\
97 &= 3 \cdot 30 + 7 \\
30 &= 4 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

so $\gcd(127, 97) = 1$. This implies that the equation has a solution. To get a solution, let's "solve" the remainders from the equations above using 127 and 97 and starting from the bottom:

$$\begin{aligned}
1 &= 7 - 3 \cdot 2 \\
&= 7 - 3 \cdot (30 - 4 \cdot 7) = -3 \cdot 30 + 13 \cdot 7 \\
&= -3 \cdot 30 + 13 \cdot (97 - 3 \cdot 30) = 13 \cdot 97 - 42 \cdot 30 \\
&= 13 \cdot 97 - 42 \cdot (127 - 97) = -42 \cdot 127 + 55 \cdot 97.
\end{aligned}$$

From this we see that a solution to $97x + 127y = 1$ is $x = 55$ and $y = -42$.

Exercise 3. Simplify the fraction

$$\frac{260\,712}{561\,752}$$

Solution. We can simplify the fraction by dividing the numerator and denominator by a number that's a factor of both. We could calculate the greatest common divisor of both, or do it little by little. For example we see immediately that both 260 712 and 561 752 are even (they end in a '2'), so we could start by dividing by 2. However let's calculate the greatest common divisor to practice that skill:

$$\begin{aligned}
561\,752 &= 2 \cdot 260\,712 + 40\,328 \\
260\,712 &= 6 \cdot 40\,328 + 18\,744 \\
40\,328 &= 2 \cdot 18\,744 + 2\,840 \\
18\,744 &= 6 \cdot 2\,840 + 1\,704 \\
2\,840 &= 1 \cdot 1\,704 + 1\,136 \\
1\,704 &= 1 \cdot 1\,136 + 568 \\
1\,136 &= 2 \cdot 568 + 0.
\end{aligned}$$

Hence $\gcd(260\,712, 561\,752) = 568$. This is the largest number that divides both the numerator and denominator. Hence the fraction simplifies to

$$\frac{260\,712}{561\,752} = \frac{260\,712/568}{561\,752/568} = \frac{459}{989}.$$

Several students who used the calculator for simplifying the fraction got

$$\frac{32589}{70219}$$

as their answer. This is not the final form. It makes me think that the calculator does not calculate the gcd of the numbers, but instead guesses integers that will divide both numbers. It guessed 8 correctly, but not 71. (The gcd is $8 \cdot 71$.)

Exercise 4. A number l is called a common multiple of m and n if both m and n divide l. There are many such l. The smallest positive one is called the **least common multiple** of m and n and is denoted by $\operatorname{lcm}(m,n)$. For example $30 = \operatorname{lcm}(10,6)$ because $30 = 3 \cdot 10 = 5 \cdot 6$ (so it's a common multiple), and any smaller multiple of 10 is not a multiple of 6.

(a) Find $\operatorname{lcm}(8,12)$, $\operatorname{lcm}(20,30)$, $\operatorname{lcm}(51,68)$, $\operatorname{lcm}(23,18)$.

(b) Compare the value of $\operatorname{lcm}(m,n)$ with the values of m, n and $\gcd(m,n)$. In what way are they related? No need to prove this. Just describe it.

(c) Compute $\operatorname{lcm}(301337, 307829)$ using the formula you found in (b). You probably need a calculator for this.

Solution.

(a) Let's look at the multiples of the numbers, starting from the smaller ones.

Multiples of 8 and 12:

$$8, 16, \mathbf{24}, \dots$$
$$12, \mathbf{24}, \dots$$

hence $\operatorname{lcm}(8,12) = 24$.

Multiples of 20 and 30:

$$20, 40, \mathbf{60}, \dots$$
$$30, \mathbf{60}, \dots$$

hence $\operatorname{lcm}(20,30) = 60$.

Multiples of 51 and 68:

$$51, 102, 153, \mathbf{204}, \dots$$
$$68, 136, \mathbf{204}, \dots$$

hence $\operatorname{lcm}(51,68) = 204$.

Multiples of 23 and 18:

$$23, 46, 69, 92, 115, 138, 161, 184, 207, 230, 253, 276, 299,$$
$$322, 345, 368, 391, \mathbf{414}, \dots$$
$$18, 36, 54, 72, 90, 108, 126, 144, 162, 180, 198, 216, 234, 252,$$
$$270, 288, 306, 324, 342, 360, 378, 396, \mathbf{414}, \dots$$

hence $\operatorname{lcm}(23,18) = 414$.

(b) Let's investigate lcm and gcd for small numbers, like 4 and 6. We have $\gcd(4,6) = 2$ because $4 = 2^2$ and $6 = 2 \cdot 3$. The multiples of 4 and 6 are:

$$4, 8, \mathbf{12}, \ldots$$
$$6, \mathbf{12}, \ldots$$

so $\operatorname{lcm}(4,6) = 12$.

Let's try another pair of small numbers: 1 and 2. Then $\gcd(1,2) = 1$ and $\operatorname{lcm}(1,2) = 2$.

Our observations:

pair	lcm	gcd
$(4,6)$	12	2
$(1,2)$	2	1

We notice that the multiplication of the original numbers looks like the same as the multiplication of lcm and gcd. Let's test our hypothesis: we saw that $\operatorname{lcm}(8,12) = 24$. The gcd is 4. Then $\operatorname{lcm}(8,12) \cdot \gcd(8,12) = 24 \cdot 4 = 96$. On the other hand $8 \cdot 12 = 96$ too. It looks like

$$\operatorname{lcm}(m,n) \cdot \gcd(m,n) = mn.$$

(c) To calculate $\operatorname{lcm}(301\,337, 307\,829)$ let's use the formula above. Hence we must calculate the gcd of the numbers.

$$\begin{aligned}
307\,829 &= 1 \cdot 301\,337 + 6\,492 \\
301\,337 &= 46 \cdot 6\,492 + 2\,705 \\
6\,492 &= 2 \cdot 2\,705 + 1\,082 \\
2\,705 &= 2 \cdot 1\,082 + 541 \\
1\,082 &= 2 \cdot 541
\end{aligned}$$

so the $\gcd(301\,337, 307\,829) = 541$. Then

$$\begin{aligned}
\operatorname{lcm}(301\,337, 307\,829) &= \frac{301\,337 \cdot 307\,829}{\gcd(301\,337, 307\,829)} = \frac{301\,337 \cdot 307\,829}{541} \\
&= 301\,337 \cdot \frac{307\,829}{541} = 301\,337 \cdot 569 = 171\,460\,753.
\end{aligned}$$

Exercise 5. What is the last digit of 7^{2023}?

Solution. We find the last digit by looking at the number modulo 10. Let's see if there's anythin useful in the powers of 7 modulo 10:

$$\begin{aligned}
&7^1 \equiv 7 \pmod{10}, \\
&7^2 \equiv 49 \equiv 9 \pmod{10}, \\
&7^3 \equiv 7^2 \cdot 7 \equiv 9 \cdot 7 \equiv 63 \equiv 3 \pmod{10}, \\
&7^4 \equiv 7^3 \cdot 7 \equiv 3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}.
\end{aligned}$$

This means that every 4th power can be "cancelled out". Namely, in arithmetic modulo 10 we have $7^4 \equiv 1$. For example

$$7^{2023} \equiv 7^4 \cdot 7^{2019} \equiv 7^{2019} \pmod{10}.$$

Continuying simiarly we see that

$$7^{2023} \equiv \underbrace{7^4 \cdot 7^4 \cdot \ldots \cdot 7^4}_{2020/4 = 505 \text{ factors } 7^4} \cdot 7^3 \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{505 \text{ ones}} \cdot 7^3 \equiv 2 \pmod{10}.$$

So the last digit is 3.

Another, shorter and less explanatory solution is:

$$7^{2023} \equiv (7^2)^{1011} \cdot 7 \equiv 49^{1011} \cdot 7 \equiv (-1)^{1011} \cdot 7 \equiv -1 \cdot 7 \equiv -7 \equiv 3 \pmod{10}.$$

Exercise 6. Find all integer solutions (x, y) to $6x - 13y = 5$.

Solution. Let's confirm if there are solutions: $\gcd(6, 13) = 1$ and $1 \mid 5$, so there are solutions. To find all the solutions let's write the equation as a congruence.

Assume that (x, y) is an integer solution. Then $13y = -5 + 6x$, so by the definition of congruence we have $13y \equiv -5 \pmod 6$. But we have $13 \equiv 1 \pmod 6$, so $-5 \equiv 13y \equiv y \pmod 6$. This means that if (x, y) is an integer solution, then $y = 6k - 5$ for some $k \in \mathbb{Z}$. Let's then solve for x by using this formula for y:

$$\begin{aligned} 6x - 13y = 5 \text{ and } y = 6k - 5 &\implies 6x - 13 \cdot (6k - 5) = 5 \\ &\implies 6x - 13 \cdot 6k + 65 = 5 \\ &\implies 6x = 13 \cdot 6k - 60 \\ &\implies x = 13k - 10. \end{aligned}$$

We have shown that if $x, y \in \mathbb{Z}$ and $6x - 13y = 5$ then there is $k \in \mathbb{Z}$ such that

$$\begin{cases} x = 13k - 10 \\ y = 6k - 5 \end{cases}. \tag{1}$$

Let's see if all such numbers are solutions. Firstly, if $k \in \mathbb{Z}$ then x and y as written above are integers. Secondly then

$$6x - 13y = 6 \cdot 13k - 60 - 13 \cdot 6k + 65 = 5$$

so they solve the equation. Hence all the solutions and only the solutions are given by the formula (1) where k can be any integer.

Note: if we had written the equation $6x - 13y = 5$ as a congruence in the form $6x \equiv 5 \pmod{13}$ we would have required an extra step. We would have had to multiply the congruence by the "multiplicative inverse of 6 modulo 13" which is 11 (because $11 \cdot 6 = 66 = 65 + 1 = 5 \cdot 13 + 1$). This is a very useful concept, because then $11 \cdot 6x \equiv 66x \equiv x \pmod{13}$. To continue, if $6x \equiv 5 \pmod{13}$ then $x \equiv 66x \equiv 55 \equiv 3 \pmod{13}$. This gives the solution $x = 13m + 3$, $m \in \mathbb{Z}$. This is equivalent to the solution $x = 13k - 10$, $k \in \mathbb{Z}$ by the substitution $m = k - 1$.