Worksheet 5: Number Theory

Question 1. Write at least one divisor (not equal to 1 and to N) for the following numbers:
(A) $N = 2^{48} + 1$
(B) $N = 2^{77} - 1$
(C) $N = 41^4 + 4$.
Write your answer as three comma-separated numbers arithmetic expressions.
Note. You may want to use various algebraic identities to factorize:

$$a^n - b^n =$$
$$=(a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right)$$
$$a^{2n+1} + b^{2n+1} =$$
$$=(a+b)\left(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n}\right)$$
$$a^4 + 4b^4 =$$
$$=(a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$$

Question 2. Are these statements true or false ('all integers" include also negative numbers):

(A) For all integers a, b, c, if $a \mid b$ and $a \mid c$, then $a \mid \gcd(b, c)$.

(B) For all integers a, b, c, if $a \mid \gcd(b, c)$, then $a|b$ and $a|c$.

(C) For all integers a, b, c, d, if $a \mid b$ and $c \mid d$, then $ac \mid \operatorname{lcm}(b, d)$.

(D) For all integers a, b, c, $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

(E) For all integers a, b, c, $\operatorname{lcm}(\gcd(a, b), c) = \gcd(\operatorname{lcm}(a, c), \operatorname{lcm}(b, c))$.

(F) For all primes $p > 2$, $2^p + 1$ is not a prime.

Write your answer as a comma-separated string of T/F. For example, `T,T,T,T,T,T`.
Note. Even though you only write the answers, make sure that you are able to justify your answer. For true statements you should be able to find a reasoning; for false ones – a counterexample.

Question 3. Find $\gcd(2160^{20}, 150^{30})$
Write your answer as a product of prime powers `p^a*q^b*r^c` or similar. Numbers p, q, r etc. should be in increasing order. All exponents (even those equal to 1) should be written explicitly.

Question 4. Convert $(101\,0110\,0111)_2$ to base 16, base 8 and base 4.
Write your answer as 3 comma-separated numbers. For the hexadecimal notation use all digits and also capital letters A,B,C,D,E,F.

Question 5. Find the sum and the product of these two integers written in ternary: $(110112)_3$, $(1000221)_3$.

Write your answer as two comma-separated numbers (both written in binary).
Note. You may want to try the addition and multiplication algorithm directly in ternary system (without converting them into the decimal and back).

Question 6. Write the fraction $1/7$ as an infinite periodic binary fraction.
Note. One method to get, say, the first 16 digits of this fraction, you can multiply $1/7$ by $2^{16} = 65536$ and then express $65536/7 = 9362, \ldots$ in binary. A more efficient way is to use the regular division algorithm ("long division", "dalīšana stabiņā"); this allows to generate a sequence of binary digits of unlimited length.
Write your answer as `0.(...)` or `0....(...)`.
(I.e. you start by the integer part, then write all digits preceding the period, then the perdiod itself in round parentheses.)

Question 7. Write the first eight powers (with non-negative exponents) of number 5 modulo 21: $5^0, 5^1, 5^2, 5^3, \ldots, 5^7$.
Write your answer as a comma-separated list of eight remainders (mod 21), – all are numbers between 0 and 20.

Question 8. Find the inverse values $1^{-1}, \ldots, 10^{-1}$ modulo 11. (The inverse number of x modulo 11 is x^{-1} such that $x^{-1}x \equiv 1 \pmod{11}$.)
Write your answer as 10 comma-separated numbers.

Question 9. Find the smallest three positive integer values of x that are solutions of the equation $55x + 21y = 1$.
Write your answer as three comma-separated integers.

Answers

Question 1. Answer: `2^16+1,2^7-1,5`

(A) $N = 2^{48} + 1 = \left(2^{16} + 1\right)\left(2^{32} - 2^{16} + 1\right)$.
(B) $N = 2^{77} - 1 = \left(2^{7} - 1\right)\left(2^{70} + 2^{63} + \ldots + 1\right)$.
(C) $N = 41^4 + 4$ ends with 5, so it is divisible by 5. Also $N = \left(41^2 + 2 \cdot 41 + 2\right)\left(41^2 - 2 \cdot 41 + 2\right)$.
Expressions in form $x^4 + 4y^4$ can be factorized using Sophie Germain identity. See https://bit.ly/2xkJeq1.

Question 2. Answer: `T,T,F,T,T,T`
(A) $((a \mid b) \wedge (a \mid c)) \rightarrow a \mid \gcd(b, c)$
`True`. That's the definition of GCD: Any common divisor a also divides $\gcd(b, c)$.
(B) $(a \mid \gcd(b, c)) \rightarrow (a|b \wedge a|c)$
`True`. Obviously $\gcd(b, c)$ divides both b and c.
(C) $(a \mid b \wedge c \mid d) \rightarrow (ac \mid \operatorname{lcm}(b, d))$.
`False`. We can take $a = 2^3$, $b = 2^4$, $c = 2^5$, $d = 2^6$. Then $\operatorname{lcm}(b, d) = 2^6$.
(D) $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.
`True`. Both sides represent the GCD of all three numbers.
(E) $\operatorname{lcm}(\gcd(a, b), c) = \gcd(\operatorname{lcm}(a, c), \operatorname{lcm}(b, c))$.
`True`. Take any prime factor that participates in the numbers

$$\begin{cases} a = p^i \cdot \ldots \\ b = p^j \cdot \ldots \\ c = p^k \cdot \ldots \end{cases}$$

Then both sides are divisible by p^m, where

$$m = \max(\min(a, b), c) = \min(\max(a, c), \max(b, c)).$$

(F) For all primes $p > 2$, $2^p + 1$ is not a prime.
`True`. All such numbers are divisible by 3, if p is an odd number.

Question 3. Answer: `2^30*3^30*5^20`
Express both numbers as a product of their prime factors.

$$\begin{aligned} &\gcd\left((2^4 \cdot 3^3 \cdot 5)^{20},\ \ (2^1 \cdot 3^1 \cdot 5^2)^{30}\right) = \\ =&\gcd\left(2^{80} \cdot 3^{60} \cdot 5^{20},\ \ 2^{30} \cdot 3^{30} \cdot 5^{60}\right) = \\ =&2^{30} \cdot 3^{30} \cdot 5^{20} \end{aligned}$$

Question 4. Answer: TBD

Question 5. Answer: TBD

Question 6. Answer: TBD

Question 7. Answer: TBD

Question 8. Answer: TBD

Question 9. Answer: TBD