Quiz 5: Number Theory

Question 1. Do the prime factorization for this 6-digit positive integer: 510, 510.

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 2. Are these statements true or false (do not forget that "all integers" include also negative numbers):

(A) For all integers a, b, c, if $a|c$ and $b|c$, then $(a+b)|c$.

(B) For all integers a, b, c, d, if $a|b$ and $c|d$, then $(ac)|(b+d)$.

(C) For all integers a, b, if $a|b$ and $b|a$, then $a = b$.

(D) For all integers a, b, c, if $a|(b+c)$, then $a|b$ and $a|c$.

(E) For all integers a, b, c, if $a|bc$, then $a|b$ or $a|c$.

(F) If p and q are primes (> 2), then $pq + 1$ is never 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 $\mathrm{lcm}(24^{75}, 75^{24})$

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 $(100\,1100\,0011)_2$ to base 16, base 8 and base 7.

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. Express the infinite periodic binary fraction $0.0001100110011\ldots_2 = 0.0(0011)$ as a rational number.
Note 1. In binary fractions a digit that is k places after the point is multiplied by 2^k. For example, 0.1_2 means $1/2$; 0.01_2 means $1/4$ and so on.
Note 2. You may need to use infinite geometric progression to find its value.

Write your answer as `P/Q`, where P, Q are both in decimal notation.

Question 6. Find the sum and the product of these two integers written in binary: $(101011)_2$, $(1101011)_2$.
Note. You may want to try the addition and multiplication algorithm directly in binary (without converting them into the decimal and back to the binary).

Write your answer as two comma-separated numbers (both written in binary).

Question 7. Write the first 10 powers of number 3 modulo 11: $3^1, 3^2, 3^3, \ldots, 3^{10}$.

Write your answer as a comma-separated list of ten remainders (mod 11), – numbers between 0 and 10.

Question 8. Alice has only 21-cent coins, Bob has 34-cent coins. Alice wants to pay Bob exactly 1 cent. Find two non-negative integers s, t that satisfy $21s - 34t = 1$.

Write your answer as two comma-separated integers.

Question 9. Consider the opposite situation: Alice has only 34-cent coins, Bob has only 21-cent coins. Find two non-negative integers s, t that satisfy $34s - 21t = 1$.

Write your answer as two comma-separated integers.

Question 10. Find 21^{-1} modulo 34. (This is a number z between 0 and 33 such that $21z \equiv 1 \pmod{34}$.)

Write your answer as a number modulo 34 (i.e. between 0 and 33).

Question 11. Solve the congruence equation $21x \equiv 11 \pmod{34}$.

Write your answer as a number modulo 34 (i.e. between 0 and 33).

Question 12. Solve the Bezout identity for the numbers $a = 390, b = 72$: Find any integers x, y satisfying the equation $390x + 72y = \gcd(390, 72)$.

Write your answer as two comma-separated integers.

Answers

Question 1.
Answer: `2^1*3^1*5^1*7^1*11^1*13^1*17^1`
When factorizing a number with computer, try dividing it by small primes $2, 3, 5, 7, \ldots$ (if divisible, then divide by that prime, and try to divide by that prime again, and by all larger primes). Do so, until you reacn $\sqrt{n}$.

If you wish to factorize large "symmetric-looking" numbers even faster (where the same fragment repeats itself many times), notice that $510510 = 510 \cdot 1001$. Then factorize each of these numbers separately.

Question 2. Answer: `F,F,F,F,F,T`
(A) $2 \mid 6$ and $3 \mid 6$, but $(2+3) \nmid 6$ (i.e. 5 does not divide 6).
(B) $2 \mid 2$ and $3 \mid 3$, but $(2 \cdot 3) \nmid (2+3)$ (i.e. 6 does not divide 5).
(C) For positive a, b this would be true, but for $\mathbb{Z}$ it is not: $2 \mid (-2)$ and $(-2) \mid 2$, but $2 \neq -2$. **(D)** $5 \mid (3+7)$, but $5 \nmid 3$ and also $5 \nmid 7$; so you can make even both conclusions fail, not just one of them. **(E)** $6 \mid 2 \cdot 15$, but $6 \nmid 2$ and also $6 \nmid 15$. (This statement $(a|bc) \to ((a|b) \vee (a|c))$ would be true iff a is a prime number. Then it is called *Euclid's Lemma*. But it is false for all non-prime a). **(F)** The last statement is true, because $pq + 1$ would be an even number bigger than 2, so it cannot be prime.

We summarize, that all statements can have counterexamples, but the last one is always true.

Question 3. Answer: `2^225*3^75*5^48`
$\mathrm{lcm}(24^{75}, 75^{24}) = \mathrm{lcm}(2^{225} \cdot 3^{75}, 3^{24} \cdot 5^{48})$. Then take the maximal values for each prime power 2^a, 3^b, 5^c in both numbers.

Question 4. Answer: `4C3,2303,3361`
Hexadecimal notation can be obtained, if we group digits by four (from the end of the number): `100:1100:0011`. Encode each group of digits: `4C3`.
Octal notation can be obtained as we group digits by three: `10:011:000:011`. Encode each group: `2303`.
Decimal notation is $4 \cdot 16^2 + \mathtt{C} \cdot 16^1 + 3 = 4 \cdot 256 + 12 \cdot 16 + 3 = 1219$. We can divide 1219 by 7 and each time record the remainder:

```
1219:7 = 174, R.1
174:7 = 24, R.6
24:7 = 3, R.3
3:7 = 0, R.3
```

Write all the remainders from right to left: `3361`. This is the representation of 1219 in base 7. You can check this by Horner's scheme:

$$((((3) \cdot 7 + 3) \cdot 7 + 6) \cdot 7 + 1) = 1219.$$

Question 5. Answer: `1/10`

$$\alpha = 0.0001100110011\ldots_2 = \frac{1}{2} \cdot 0.001100110011\ldots_2 =$$
$$= \frac{1}{2} \cdot 3 \cdot 0.000100010001\ldots_2 =$$
$$= \frac{3}{2} \cdot \left(\frac{1}{16} + \frac{1}{16^2} + \frac{1}{16^3} + \ldots \right).$$

Apply the formula of infinite geometric progression:

$$\left(\frac{1}{16} + \frac{1}{16^2} + \frac{1}{16^3} + \ldots \right) = \frac{\frac{1}{16}}{1 - \frac{1}{16}} = \frac{1}{15}.$$

We get $\alpha = \frac{3}{2} \cdot \frac{1}{15} = \frac{3}{30} = \frac{1}{10}$.

Note. This example has some practical implications: the floating point number 0.1 looks short and simple in decimal system. But it is an infinite periodic fraction when written in binary. Therefore it is stored with a rounding error in computer memory; doing arithmetic on such numbers may cause these errors to accumulate.

Question 6. Answer: `10010110,1000111111001`
Fastest way is adding (or multiplying) in binary notation using grid paper. If we want to double-check the result, we can convert each number into decimal:

$$101011_2 = 43_{10}; \quad 1101011_2 = 107_{10}.$$

Sum is 150 and the product is 4601. Then convert back both numbers $(150, 4601)$ into binary.

Question 7. Answer: `3,9,5,4,1,3,9,5,4,1`
Every next remainder is the previous remainder multiplied by 3 modulo 11. To avoid operating with large numbers, we immediately reduce each power $3^{k+1} = 3^k \cdot 3$ as a remainder (between 0 and 10).

These remainders form a period; after a period of 5, the remainders repeat indefinitely. (Accordingly to the *Little Fermat Theorem*, a^{10} should be congruent 1 (mod 11) for any a not divisible by 11; and after that the remainders will be periodic. So, even for other $a \neq 3$ something similar should happen.)

Question 8. Answer: `13,8`
Observe that $\gcd(21, 34) = 1$, so the numbers 21 and 34 are mutual primes. We can guess these coefficients s, t (or try out various $21s$ until it gives the remainder 1, when divided by 34). If we want to proceed by Blankinship's algorithm, it will work efficiently for any numbers:

$$\begin{pmatrix} 21 & 1 & 0 \\ 34 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 21 & 1 & 0 \\ 13 & -1 & 1 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 8 & 2 & -1 \\ 13 & -1 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 8 & 2 & -1 \\ 5 & -3 & 2 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 3 & 5 & -3 \\ 5 & -3 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 5 & -3 \\ 2 & -8 & 5 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 1 & 13 & -8 \\ 2 & -8 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 13 & -8 \\ 0 & -34 & 21 \end{pmatrix}.$$

The last two tables have one of the two rows: 1, 13, −8. This means that we are able to get number 1, by using coefficients 13 and −8 respectively:

$$21 \cdot (13) + 34 \cdot (-8).$$

Therefore $s = 13; t = -8$.

There are infinitely many other answers (you can get all of them, if you increment s by $34k$ and t by $21k$. Then both changes will cancel out:

$$(13, 8); \quad (47, 29); \quad (81, 50); \ldots$$

Question 9. Answer: `13,21` or `34,55` etc.
From the previous question we already know that $21s + 34t = 1$ for $(s, t) = (13, -8)$. In fact, there are infinitely many pairs (s, t) satisfying that equation $21s + 34t = 1$. If we decrease s by 34 and increase t by 21, then the expression does not change; then we can decrease/increase again, and so on.

Let us perform that step once: $(s_2, t_2) = (13 - 34, -8 + 21) = (-21, 13)$. Therefore $21s_2 + 34t_2 = 1$ or $21 \cdot (-21) + 34 \cdot 13 = 1$. Therefore Alice can pay with 13 34-cent coins and get back 21 21-cent coins. This would also let her pay 1 cent.

Question 10. Answer: `13`
We rewrite the solution obtained from Question 8. Since $21s - 34t = 1$ (for $s = 13, t = 8$), we can compute remainders from both sides:

$$1 = 21s - 34t \equiv 21s \pmod{34}.$$

Therefore $s = 13$ satisfies $21 \cdot s \equiv 1$.

Question 11. Answer: `7`
We know that $21^{-1} = 13 \pmod{34}$ from the previous exercise. Now we can solve the congruence equation:
$21x \equiv 11 \pmod{34}$;
$21^{-1} \cdot 21x \equiv 21^{-1} \cdot 11 \pmod{34}$;
$1x \equiv 13 \cdot 11 \pmod{34}$;
$x \equiv 143 \equiv 7 \pmod{34}$.

Question 12. Answer: `5,-27`
We can easily guess that $\gcd(390, 72) = 6$ and with some trial and error we can find that

$$390 \cdot (5) + 72 \cdot (-27) = 6.$$

To show an algorithmic way, we could do the row operations like in Blankinship's algorithm again: start from the table:

$$\begin{pmatrix} 390 & 1 & 0 \\ 72 & 0 & 1 \end{pmatrix} \rightsquigarrow \ldots$$

But let us show another (less formal) method: write the regular Euclidean algorithm (and preserve coefficients before 390 and 72):

- $30 = 390 - 5 \cdot 72$.
- $12 = 72 - 2 \cdot 30 =$
  $= 72 - 2 \cdot (390 - 5 \cdot 72) =$
  $= 11 \cdot 72 - 2 \cdot 390$;
- $6 = 30 - 2 \cdot 12 =$
  $(390 - 5 \cdot 72) - 2 \cdot (11 \cdot 72 - 2 \cdot 390) =$
  $= 5 \cdot 390 - 27 \cdot 72$.