

Here are some answers to the first exam.

1. What is the sum of all the even natural numbers that are less than or equal to 100?

A. $2 + 4 + 6 + \dots + 100 = 2 \times (1 + 2 + \dots + 50) = 2 \cdot \frac{50(50+1)}{2} = 50 \times 51.$

2. Suppose you want to plan your dinners for the next week (5 dinners). There are ten different dishes that you know how to prepare, which is good because you don't ever want to eat the same thing twice in the same week. How many different meal plans could you create under these conditions?

B. $10 \times 9 \times 8 \times 7 \times 6$. To count the possibilities you could draw a tree that branches out on 5 levels, showing the possible answers to the questions "What will I cook Monday?" (10 answers), "What will I cook Tuesday?" (9 answers), etc.

3. As in the previous problem let's suppose you can cook ten different dinners. Suppose you cook ALL of them, one day at a time, starting on a Monday. Then you spend another 10 days, again cooking a different one of your favorite dishes every night. (You cook them in a different order in the second set so your palate does not get bored!) Repeat this a grand total of 12 times (i.e. each dish will be cooked 12 times). On which day of the week will you be cooking your Last Supper?

A. Monday. You will cook a for a total of $10 \times 12 = 120$ days; that works out to 17 weeks and one day, i.e. $120 \equiv 1 \pmod{7}$. You don't even have to do much arithmetic here: $10 \times 12 \equiv 3 \times 5 = 15 \equiv 1$. (Why is a 10-day cycle "the same" as a 3 day cycle? Why is 12 cycles "the same" as 5 cycles?)

Anyway, you end on day number 120, which is the same day of the week as days number 113, 106, ..., 8, 1 because they are all congruent to each other mod 7. And day number 1 was a Monday, so day 120 will be Monday too.

I gave credit to those who did all the math right and then mis-interpreted this, thinking they were moving forward one day to Tuesday. But don't count on such generosity in the future!

4. Compute $2^{64} \pmod{31}$, that is, tell me which of these is congruent to 2^{64} , modulo 31:

C. 16 You could have computed $2^{64} = 2^{31} \cdot 2^{31} \cdot 2^2 \equiv 2 \cdot 2 \cdot 4 = 16$ using Fermat's theorem. Or you could have noted that $2^5 = 32 \equiv 1$ so that $2^{64} = (2^5)^6 \cdot 2^4 \equiv 1^6 \cdot 16 = 16$. Or you could have worked out the first half-dozen or so powers of 2 (modulo 31) and noticed the pattern was starting to cycle.

5. Today I decide to encrypt my messages using our standard base-29 encoding scheme (A=1, B=2, etc.) and encrypting my messages by multiplying each letter by 10. If you intercept an encrypted message that contains the string "AJZ" (that is, the message contains the sequence 1, 10, 26), what was the original message string?

B. CAT . If we are working mod 29, multiplication-by-10 is undone by multiplication-by-3 since $3 \cdot 10 \equiv 1 \pmod{29}$. So the original message must have been $3 \cdot 1 = 3, 3 \cdot 10 = 30 \equiv 1, 3 \cdot 26 = 78 \equiv 49 \equiv 20$; that's 3=C, 1=A, 20=T.

6. Which numbers in the following list are rational?

$$w = \sqrt{5}, \quad y = \sqrt{100} \quad z = \sqrt{3} \quad a = w \times z \quad b = w \times y \quad c = w \times w$$

B. y, c are both rational: $y = 10$ and $c = 5$. None of the others are because they are rational numbers times an irrational square root ($w = \sqrt{5}, z = \sqrt{3}, a = \sqrt{15}, b = 10\sqrt{5}$)

7. In the card game Set, a winning “set” is formed by three cards $A, B,$ and C . cards A and B are shown on the next page; what can C be?

Ans: The card with one clear green oval

8. Suppose after I grade this exam I announce “Everyone got some problem wrong.” That sentence is ambiguous; it could mean either of the two ideas expressed mathematically below. Restate in ordinary English what each of these sentences say. (Your answers should make it clear to an ordinary English speaker why A and B say different things!)

A. $\forall x \exists y$ (person x missed problem y) Everyone missed at least one problem (possibly different problems for different people)

B. $\exists y \forall x$ (person x missed problem y) There’s a (hard) problem that everyone missed.

Here are the extra-credit ones:

C. $\exists x \forall y$ (person x missed problem y) Someone scored a zero

D. $\forall y \exists x$ (person x missed problem y) For each problem there was at least one person who missed that problem.

E. $\exists x \exists y$ (person x missed problem y) At least one person got less than 100%

F. $\forall x \forall y$ (person x missed problem y) Everyone got a zero. (Hardest test ever!)

9. The *Triangular numbers* are the numbers in the sequence 1, 3, 6, 10, 15, ... The n th triangular number may be computed from the formula $T_n = \frac{n(n+1)}{2}$.

Notice that, at least with the numbers shown, when you add two consecutive triangular numbers together, you get a perfect square: $1 + 3 = 2^2$, $10 + 15 = 5^2$, etc. Explain why this will always be true. That is, show me that if you add the n th triangular number to the next triangular number in the list after it, you will get a perfect square. (Use algebra.)

Ans: Do as I asked: add the n th triangular number to the one after it (which would be the $(n + 1)$ st one); you will get

$$T_n + T_{n+1} = \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} = \frac{(n+1)}{2} \cdot (n + (n+2)) = \frac{(n+1)}{2} \cdot (2n+2) = (n+1)^2$$

which is, obviously, a perfect square.

Other types of explanations can be made to work too, with lots of variety in how they are stated. For example some of you noted that each $T_n = T_{n-1} + n$ so if you already know that $T_n + T_{n-1} = n^2$ then the next example to compute, that is, $T_{n+1} + T_n$, will be larger by $(n + 1) + n = 2n + 1$; but $n^2 + (2n + 1)$ is exactly $(n + 1)^2$ as noted above. Or you could recall that T_n is our formula for $1 + 2 + \dots + n$, so if you add T_n to T_{n+1} you’re actually computing (in a different order) the sum

$$(1 + n) + (2 + (n - 1)) + (3 + (n - 2)) + \dots + (n + 1) + ((n + 1) + 0),$$

which is a total of $n + 1$ $(n + 1)$'s, i.e. $(n + 1)^2$. There's a picture to illustrate this, showing a bunch of dots in a $(n + 1)$ -by- $(n + 1)$ grid; draw a diagonal through the middle and you'll see two consecutive triangular numbers adding up to a perfect square.

10. Show that 0-372-02763-6 is a valid ISBN. Then circle any two adjacent digits in this code, swap them, and show that the resulting code is NOT a valid ISBN.

Ans: We need to compute $(1 \times 0) + (2 \times 3) + (3 \times 7) + \dots (10 \times 6) \pmod{11}$; the ISBN is valid iff this is zero $(\pmod{11})$. The actual total is 231 but I hope you reduced everything $\pmod{11}$ as you went along; for example I computed this number $\pmod{11}$ as $0 + 6 + (-1) + 8 + 0 + 1 + 5 + 4 + 5 + 5 = 33 \equiv 0$.

If you swap the i th and j th digits (adjacent or not), and if those digits are a and b respectively, you will replace the two terms $i \times a$ and $j \times b$ with $j \times a$ and $i \times b$ respectively. That means your ISBN sum will go up by $(j - i) \cdot a + (i - j) \cdot b = (i - j)(a - b)$. This will NEVER be zero $(\pmod{11})$ unless one of the factors is; but $i - j \neq 0$ because we are swapping digits from different positions, and $a - b \neq 0$ because we are swapping digits that are different. (No one will notice if you swap the two 3's!) That's the nice thing about this ISBN procedure: it will catch you if you accidentally make just a single dyslexic swap.

11. Suppose I decide to encode my messages using 26 letters and FOUR symbols; then every character can again be expressed as a number but we would do all of our computations modulo 30 instead of modulo 29.

Explain why we cannot use an encryption system that replaces each number x with the encrypted form $y \equiv 10x \pmod{30}$. Something will go wrong – do you see what it is?

Ans: The difference between this situation and our usual encryption is that 30 is NOT prime, and in fact it has a divisor in common with the multiplier (10) that we are using for encryption. That's bad along several fronts:

1. You won't be able to find a "reciprocal", i.e. a number m that you can multiply by to decrypt, because the congruence $10m \equiv 1 \pmod{30}$ is not true for any m . (All the numbers you work with will end in a 0, not a 1.)

2. You are losing information when you encrypt. For example the letters A and D (i.e. the numbers 1 and 4) will both encrypt to the number 10 (i.e. to the letter J) because $10 \times 4 = 40 \equiv 10 \pmod{30}$. So how could your interlocutor decrypt the J? – He or she wouldn't know if the original letter was an A or a D.

3. Your encrypted messages look silly. After all, the only encryptions you will get will be letters $y = 10x \pmod{30}$, which are $y = 10, 20, 30$; those are the letter J and T and the new punctuation mark (maybe it was "!") and so a typical encrypted message would say "JT!TTJTJ!!!JT!TT!" There's not a lot of information hidden in there...