Applied Algebra

Instructions Please answer these questions on your own paper. Explain your work in complete sentences.

1. Determine the smallest positive integer n with the property that there exist integers x and y such that $60x + 42y = n$.

   Solution. The statement describes the greatest common divisor of 60 and 42. Since $60 = 2^2 \times 3 \times 5$, and $42 = 2 \times 3 \times 7$, the greatest common divisor of 60 and 42 equals 2×3. Thus $n = 6$.

2. Prove by induction that

   $$(1! \cdot 1) + (2! \cdot 2) + \cdots + (n! \cdot n) = (n+1)! - 1$$

   for every positive integer n (where, as usual, the factorial $n!$ means the product of all the integers between 1 and n inclusive).

   Solution. When $n = 1$, the statement is valid because $1! \cdot 1 = 1$ and $(1+1)! - 1 = 2 - 1 = 1$. Thus the basis step of the induction holds.

   Suppose it is known that

   $$(1! \cdot 1) + (2! \cdot 2) + \cdots + (k! \cdot k) = (k+1)! - 1$$

   for a certain positive integer k. Adding $(k+1)! \cdot (k+1)$ to both sides shows that

   $$\begin{aligned} &1! \cdot 1 + 2! \cdot 2 + \cdots + k! \cdot k + (k+1)! \cdot (k+1) \\ &\qquad = (k+1)! - 1 + (k+1)! \cdot (k+1) \\ \text{(factoring)} &\qquad = (k+1)!(1 + (k+1)) - 1 \\ &\qquad = ((k+1)+1)! - 1. \end{aligned}$$

   Therefore the statement for integer $k+1$ is a consequence of the statement for integer k. By mathematical induction, the statement holds for every positive integer.

3. When the number $65^{93} \times 56^{39}$ is written out, it has 237 digits. How many zeroes are there at the right-hand end? Explain how you know.

   Solution. Since $65 = 5 \times 13$ and $56 = 7 \times 8$, the number has the prime factorization $2^{117} \times 5^{93} \times 7^{39} \times 13^{93}$. The number is divisible by 10^{93} but not by any larger power of 10, so there are 93 zeroes at the end.

4. Find a multiplicative inverse of 23 modulo 31.

   Solution. Here is a matrix implementation of the Euclidean algorithm:

$$\begin{pmatrix} 1 & 0 & 31 \\ 0 & 1 & 23 \end{pmatrix} \xrightarrow{R1 \to R1 - R2} \begin{pmatrix} 1 & -1 & 8 \\ 0 & 1 & 23 \end{pmatrix} \xrightarrow{R2 \to R2 - 3R1} \begin{pmatrix} 1 & -1 & 8 \\ -3 & 4 & -1 \end{pmatrix}$$

   Multiply the bottom row by -1 to see that $3 \times 31 + (-4) \times 23 = 1$. Therefore -4 is one multiplicative inverse of 23 modulo 31. An equivalent positive answer is $-4 + 31$ or 27. The set of all possible answers is the congruence class $[27]_{31}$.

5. Solve the pair of simultaneous linear congruences

$$\begin{cases} x \equiv 6 \mod 7, \\ x \equiv 5 \mod 17. \end{cases}$$

   Solution. The numbers are small enough that you could find a solution by brute force. The first congruence says that x can be found in the list of numbers 6, 13, 20, 27, . . . ; the second congruence says that x can be found in the list of numbers 5, 22, 39, 56, . . . ; you need to write out enough terms to find a number that belongs to both lists.

   The thematic method, however, is to start by writing 1 as an integral linear combination of 7 and 17. Here is the relevant matrix computation:

$$\begin{pmatrix} 1 & 0 & 17 \\ 0 & 1 & 7 \end{pmatrix} \xrightarrow{R1 \to R1 - 2R2} \begin{pmatrix} 1 & -2 & 3 \\ 0 & 1 & 7 \end{pmatrix} \xrightarrow{R2 \to R2 - 2R1} \begin{pmatrix} 1 & -2 & 3 \\ -2 & 5 & 1 \end{pmatrix}$$

   Thus $-2 \times 17 + 5 \times 7 = 1$. Consequently, $-2 \times 17 \equiv 1 \mod 7$, and $5 \times 7 \equiv 1 \mod 17$. It follows that $6 \times (-2) \times 17 + 5 \times 5 \times 7$ is one solution for x. This value simplifies to -29. The set of all solutions is the congruence class $[-29]_{119}$, or, equivalently, $[90]_{119}$.

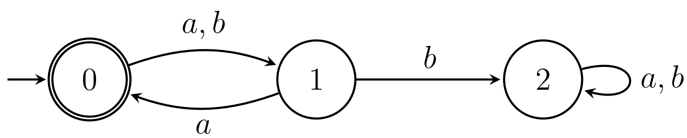
6. Using the RSA system, I encoded my birthday (month and day) in two blocks as 30 5. The public key is the pair $(33, 7)$, where 33 is the base n and 7 is the exponent a. When is my birthday?

Applied Algebra

Solution. The decoding exponent is a multiplicative inverse of 7 mod $\phi(33)$, and $\phi(33) = \phi(3 \times 11) = \phi(3) \times \phi(11) = 2 \times 10 = 20$. Evidently $3 \times 7 \equiv 1 \mod 20$, so 3 is the decoding exponent.

Now $30^3 \equiv (-3)^3 \equiv -27 \equiv 6 \mod 33$, so the first block decodes to 6. Moreover, $5^3 \equiv 125 \equiv 26 \mod 33$, so the second block decodes to 26. My birthday is 6/26, that is, June 26.

7. Describe the words (sequences of letters a and b) that the following finite-state automaton accepts.



Solution. The automaton accepts the empty word and also words of even length with the property that the letter a appears in positions 2, 4, 6, and so on, and the letters in the odd-numbered positions are arbitrary.

8. Let R be the relation defined on the set of positive integers by xRy if and only if $x^2 \equiv y^3 \mod 4$. Is this relation R reflexive? symmetric? transitive? Explain how you know.

Solution. The relation is not reflexive. Indeed, $3^2 = 9 \equiv 1 \mod 4$, while $3^3 = 27 \equiv 3 \mod 4$, so $3^2 \not\equiv 3^3 \mod 4$: the number 3 is not related to itself.

The relation is not symmetric. Indeed, the number 3 is related to 1 because $3^2 \equiv 1^3 \mod 4$; but 1 is not related to 3, for $1^2 \not\equiv 3^3 \mod 4$.

The relation is transitive. To see why, suppose that xRy and yRz. To show that xRz, consider two cases: the number y is either even or odd.

If y is even, then both y^2 and y^3 are divisible by 4. Therefore $x^2 \equiv y^3 \equiv 0 \mod 4$, and $0 \equiv y^2 \equiv z^3 \mod 4$. Thus $x^2 \equiv z^3 \mod 4$ (since both x^2 and z^3 are congruent to 0), so xRz.

If y is odd, then so is y^3. Since $x^2 \equiv y^3$, the number x must be odd too. The numbers x and y are therefore relatively prime to 4, so Fermat's theorem applies to them. Now $\phi(4) = 2$, so $x^2 \equiv 1 \mod 4$ and $y^2 \equiv 1$

mod 4. But yRz, so $z^3 \equiv 1 \mod 4$. Therefore $x^2 \equiv z^3 \mod 4$ (since both x^2 and z^3 are congruent to 1), so xRz.

In summary, the assumption that both xRy and yRz leads to the conclusion that xRz (whether y is even or odd). Consequently, the relation R is transitive.

Another way to look at this problem is that the relation really lives on $\mathbb{Z}_4$. This set is finite, so you can write an adjacency matrix for the relation, as follows. I use F (false) and T (true) instead of the usual 0 and 1 to avoid confusion with the elements 0 and 1 of the integers.

	[0]	[1]	[2]	[3]
[0]	T	F	T	F
[1]	F	T	F	F
[2]	T	F	T	F
[3]	F	T	F	F

The matrix reveals that the relation is not reflexive (because not all the entries on the main diagonal are "T") and not symmetric (because the $([1],[3])$ entry does not match the $([3],[1])$ entry). Checking transitivity still requires the examination of cases.

9. State the Chinese Remainder Theorem.

Solution. See page 54 in the textbook.