Factor puzzles from definition to applications [version 1; peer review: awaiting peer review]

Raghib Abusaris¹, KIFAH ALHAMI²

¹Department of Epidemiology and Biostatistics, King Saud bin Abdulaziz University for Health Sciences, Ar Rimayah, Riyadh, 14611, Saudi Arabia
²MATHEMATICS, AJMAN UNIVERSITY, AJMAN, 346, United Arab Emirates

Abstract
Background: Factor puzzles are a salient tool that has been consigned to oblivion.
Methods: In this paper, we introduce factor puzzles and study the existence and uniqueness of solutions along with their connections to other areas of mathematics and real-world applications.
Results: Using concepts from elementary number theory, we prove several theorems pertinent to the existence and uniqueness of a solvable factor puzzle, and the number of solutions. Furthermore, we established connections between factor puzzles and polynomial as well as matrix factorizations. In addition, we demonstrate the importance of factor puzzles in the real world was evidenced by an application in cryptography.
Conclusion: Factor puzzles are a prominent tool with many remarkable connections and real-world applications.

Keywords
Factor puzzles, prime numbers, relatively prime numbers, common factors, greatest common devisor, polynomials, matrices, cryptography

Open Peer Review

Any reports and responses or comments on the article can be found at the end of the article.
1. Introduction

Puzzles, due to their playful nature, have the potential to engage students. Furthermore, if they are well-designed, they can be used to engage students and introduce important concepts in any subject, particularly in mathematics. The mathematical habits of mind include pattern sniffing, experimenting, describing, tinkering, inventing, visualizing, conjecturing, and guessing. On the other hand, mathematical proficiency encompasses five intertwined strands, namely conceptual understanding, procedural fluency, strategic competence, adaptive reasoning, and productive disposition. Indeed, the main aim of this paper is to demonstrate how mathematicians think and approach problem solving through investigating factor puzzles.

In an \(m \times n\) factor puzzle, you are given an array \(A = [a_{ij}]\) of natural numbers (or integers) arranged in \(m\) rows and in \(n\) columns, and you are expected to find a solution which consists of vectors \(B = [b_i]_{1 \leq i \leq m}\) and \(C = [c_j]_{1 \leq j \leq n}\) of natural numbers such that \(a_{ij} = b_i c_j\) for \(1 \leq i \leq m\) and \(1 \leq j \leq n\). For clarity, consider the following depiction (factor puzzle A).

\[
\begin{array}{cccc}
\times & c_1 & c_2 & \ldots & c_n \\
b_1 & a_{11} & a_{12} & \ldots & a_{1n} \\
b_2 & a_{21} & a_{22} & \ldots & a_{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
b_m & a_{m1} & a_{m2} & \ldots & a_{mn} \\
\end{array}
\]

As an example, a \(2 \times 2\) factor puzzle looks like the following (factor puzzle B):

\[
\begin{array}{cc}
\times & c_1 & c_2 \\
b_1 & a_{11} & a_{12} \\
b_2 & a_{21} & a_{22} \\
\end{array}
\]

To the best of our knowledge, there is no systematic study of factor puzzles. As such, to mathematically study factor puzzles, the following questions were crystallized:

1. Under what condition(s) does a factor puzzle possess a solution?
2. How to solve a factor puzzle if it has a solution?
3. If a factor puzzle is solvable, how many solutions does it have?
4. When does a factor puzzle have a unique solution?
5. Given a number of solutions, can we construct a factor puzzle that has this number of solutions?
6. Do factor puzzles have connections to other mathematical concepts?
7. Do factor puzzles have real-world applications?

In this paper, we shall provide answers to the forgoing questions. Moreover, while our work will be focused on \(2 \times 2\) factor puzzles, the extension to larger puzzles should be clear from the context. To be precise, in Section 2.1, we address the important question of existence. In Section 2.2, we explain how to solve a factor puzzle, and establish criterion for the existence of a unique solution and develop an upper bound for the number of solutions of a factor puzzle. Connections to polynomial and matrix factorizations are demonstrated in Sections 2 and 3.

The overarching goal of cryptography is to securely communicate information. However, communicating securely, particularly sensitive information, requires encoding messages using a certain scheme. To decode a received message, the intended receiver needs the key used in encryption. It is possible, to add an extra layer of security, to mask the key by sending a factor puzzle whose solution is the key needed for decoding. This is the main purpose of Section 4.

Finally, we conclude in Section 5 by suggesting future directions.
2. Methods
In the following sections we will discuss the solvability of a factor puzzle, i.e., the existence of a solution and conditions for uniqueness, and its connection to factoring polynomials.

2.1 Proving the existence of a solution
To avoid wasting time, efforts, and resources, it is important to examine if a factor puzzle is solvable, i.e., has a solution, before attempting to solve it. To establish necessary and sufficient conditions for the solvability of a factor puzzle, we begin by considering a $2 \times 2$ factor puzzle. Furthermore, for ease for notation, we shall write it as follows:

\[
\begin{array}{cc}
\times & p & q \\
r & a & d \\
s & b & c \\
\end{array}
\]

**Theorem 2.1.** A $2 \times 2$ factor puzzle has a solution if and only if $ac = bd$, or equivalently, $\det \begin{pmatrix} a & d \\ b & c \end{pmatrix} = 0$.

**Proof.** Assume solvability. Then $a = pr, b = ps, c = qs$, and $d = qr$, and therefore $ac = prqs = psqr = bd$.

Conversely, suppose $ac = bd$. Then $a$ divides $bd$. This means that $a = \alpha \beta$ such that $\alpha$ divides $b$ and $\beta$ divides $d$. Therefore, $c = \left(\frac{d}{\beta}\right) \left(\frac{\beta}{\alpha}\right)$, and so $\frac{d}{\beta}$ and $\frac{\beta}{\alpha}$ both divide $c$. Hence, $p = \alpha, q = \frac{d}{\beta}, r = \beta$, and $s = \frac{\beta}{\alpha}$ define a solution of the given factor puzzle. \qed

**Example 2.1.** For the sake of illustration, consider the following examples.

1. Factor puzzle $D$

\[
\begin{array}{cc}
\times & p & q \\
r & 2 & 5 \\
s & 3 & 6 \\
\end{array}
\]

has no solution because $2 \times 6 = 12 \neq 15 = 3 \times 5$.

2. The following factor puzzle (E), on the other hand, has a unique solution. Namely, $p = 2, q = 3, r = 1, s = 2$, which can be obtained using the method outlined in the following section.

\[
\begin{array}{cc}
\times & p & q \\
r & 2 & 3 \\
s & 4 & 6 \\
\end{array}
\]

Whereas, the following factor puzzle (F) has two solutions. In fact, $p = 2, q = 3, r = 4, s = 14$ and $p = 4, q = 6, r = 2, s = 7$ are both solutions.

\[
\begin{array}{cc}
\times & p & q \\
r & 8 & 12 \\
s & 28 & 42 \\
\end{array}
\]

As a consequence of Theorem 2.1, we have the following general result.

**Theorem 2.2.** An $m \times n$ factor puzzle has a solution if and only if $a_{ij}a_{kl} = a_{kj}a_{il}$ for all $1 \leq i < k \leq m$ and $1 \leq j < l \leq n$.

Note that there are $\binom{m}{2} \binom{n}{2}$ $2 \times 2$ sub-arrays. However, there will be some redundancy. For example, if $m = 2$ and $n = 3$, then it suffices to check the condition for
2.2 Solving factor puzzles

Although it may be simple to prove that a factor puzzle is solvable, this does not provide an insight into how to actually solve these puzzles. In this section, we will attempt to put forward different methods that can be used for solving various puzzles.

2.2.1 Common factors

Although not efficient, one way to solve a satisfiable factor puzzle is to map it on a multiplication table.\(^4\) In contrast, a more proficient approach is investigating the common factors. To demonstrate, consider the following factor puzzle (G).

\[
\begin{array}{c c c c c}
\times & p & q \\
r & 12 & 8 \\
s & 36 & 24 \\
\end{array}
\]

Using the times table (Table 1), one solution is \(p = 6, q = 4, r = 2,\) and \(s = 6.\)

To discover other solutions, if there is any, one may need a bigger table. On the other hand, with Theorem 2.1 in mind, the common factors of 12 and 36 are 1, 2, 3, 4, 6, and 12. Furthermore, 36 divided by these common factors gives 36, 18, 12, 9, 6, and 3. Of these, only 12, 6, and 3 also divide 24. Hence, as shown below, the given factor puzzle affords three solutions (H):

\[
\begin{array}{c c c}
\times & 3 & 2 \\
4 & 12 & 8 \\
12 & 36 & 24 \\
\end{array} \quad \begin{array}{c c c}
\times & 6 & 4 \\
2 & 12 & 8 \\
6 & 36 & 24 \\
\end{array} \quad \begin{array}{c c c}
\times & 12 & 8 \\
1 & 12 & 8 \\
3 & 36 & 24 \\
\end{array}
\]

(H)

Note that the aforementioned proficient approach can be utilized to estimate the number of solutions a factor puzzle has. In fact, we have the following result.

**Theorem 2.3.** Let \(NF(x)\) denote the number of factors of \(x\) and \(k = \min \{NF(\gcd(a, b)), NF(\gcd(a, d)), NF(\gcd(b, c)), NF(\gcd(c, d))\}.\)

If a \(2 \times 2\) factor puzzle is solvable, then there are at most \(k\) solutions. Here, \(\gcd\) stands for greatest common divisor.

### Table 1. An example times table.

<table>
<thead>
<tr>
<th>(\times)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>24</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>24</td>
<td>28</td>
<td>32</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>30</td>
<td>35</td>
<td>40</td>
<td>45</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>24</td>
<td>30</td>
<td>36</td>
<td>42</td>
<td>48</td>
<td>54</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>14</td>
<td>21</td>
<td>28</td>
<td>35</td>
<td>42</td>
<td>49</td>
<td>56</td>
<td>63</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>32</td>
<td>40</td>
<td>48</td>
<td>56</td>
<td>64</td>
<td>72</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>18</td>
<td>27</td>
<td>36</td>
<td>45</td>
<td>54</td>
<td>63</td>
<td>72</td>
<td>81</td>
</tr>
</tbody>
</table>
**Proof.** First, we verify that number of common factors of \(a\) and \(b\) equals number of factors of \(\gcd(a, b)\). This follows from the fact that a common divisor of \(a\) and \(b\) divides any linear combination of \(a\) and \(b\) and, by Bézout’s theorem, \(\gcd(a, b)\) can be written as a linear combination of \(a\) and \(b\). \(^{p. 85}\)

Now, since \(p\) is a common factor of \(a\) and \(b\), \(q\) is a common factor of \(c\) and \(d\), \(r\) is a common factor of \(a\) and \(d\), and \(s\) is a common factor of \(b\) and \(c\), the result follows. \(\square\)

To illustrate Theorem 2.3, consider the following factor puzzle (I):

\[
\begin{array}{ccc}
\times & p & q \\
\hline
r & 63 & 126 \\
s & 27 & 54 \\
\end{array}
\]

(I)

Observe that the above factor puzzle is solvable \((63 \times 54 = 27 \times 126)\). Furthermore,

\[
\begin{align*}
\gcd(63, 126) &= 63 = 3^2 \cdot 7 \implies NF(\gcd(63, 126)) = 6 \\
\gcd(126, 54) &= 18 = 2 \cdot 3^2 \implies NF(\gcd(126, 54)) = 6 \\
\gcd(54, 27) &= 27 = 3^3 \implies NF(\gcd(54, 27)) = 4 \\
\gcd(27, 63) &= 9 = 3^2 \implies NF(\gcd(27, 63)) = 3
\end{align*}
\]

Hence, the above factor puzzle has at most 3 solutions. In fact, as shown below, it has 3 solutions (J).

\[
\begin{array}{ccc}
\times & 9 & 18 \\
\hline
7 & 63 & 126 \\
3 & 27 & 54 \\
\end{array}
\quad
\begin{array}{ccc}
\times & 3 & 6 \\
\hline
21 & 63 & 126 \\
9 & 27 & 54 \\
\end{array}
\quad
\begin{array}{ccc}
\times & 1 & 2 \\
\hline
63 & 63 & 126 \\
27 & 27 & 54 \\
\end{array}
\]

(J)

As a corollary of Theorem 2.3, we have the following result, which follows from the fact that 1 is the greatest common divisor between two relatively primes numbers.

**Corollary 2.1.** If one of the pairs \((a, b), (b, c), (c, d),\) or \((d, a)\) is relatively prime, then a solvable factor puzzle has a unique solution.

Moreover, utilizing Theorem 3.1, we can construct a factor puzzle with a desired number of solutions. This exemplifies an inverse problem. The following factor puzzle has \(k\) solutions for any positive integer \(k\). Additionally, there is nothing special about the number 2 in this context. In fact, any prime number can be used instead.

\[
\begin{array}{ccc}
\times & p & q \\
\hline
r & 2^{k-1} & 2^k \\
s & 2^k & 2^{k+1} \\
\end{array}
\]

(K)

2.2.2 Factoring polynomials

If we think of the numbers \(b_i\)'s and \(c_j\)'s as the coefficients of a polynomial of degrees \(m - 1\) and \(n - 1\), respectively, then the \(a_{ij}\)'s can be thought of as the coefficients of a polynomial of degree \(m + n - 2\); see the depiction below (L):

\[
\begin{array}{cccc}
\times & c_1x^{n-1} & c_2x^{n-2} & \cdots & c_n \\
\hline
b_1x^{m-1} & a_{11}x^{m+n-2} & a_{12}x^{m+n-3} & \cdots & a_{1n}x^{m-1} \\
b_2x^{m-2} & a_{21}x^{m+n-3} & a_{22}x^{m+n-4} & \cdots & a_{2n}x^{m-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
b_m & a_{m1}x^{n-1} & a_{m2}x^{n-2} & \cdots & a_{mn} \\
\end{array}
\]

(L)
The 2 \times 2 factor puzzle corresponds to factoring a quadratic equation into linear factors, the 2 \times 3 or 3 \times 2 corresponds to factoring a cubic equation into quadratic and linear factors, etc. Therefore, solving factor puzzles corresponds to factoring polynomials. For example, consider the polynomial \( f(x) = 3x^2 + 11x + 6 \). The corresponding factor puzzle is

<table>
<thead>
<tr>
<th>\times</th>
<th>p</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>3</td>
<td>11 - t</td>
</tr>
<tr>
<td>s</td>
<td>t</td>
<td>6</td>
</tr>
</tbody>
</table>

Using Theorem 2.1, this factor puzzle is solvable if \( t(11 - t) = 18 \), or \( t = 2, 9 \). Hence, we have two solutions depicted in (N):

<table>
<thead>
<tr>
<th>\times</th>
<th>c_1</th>
<th>c_2</th>
<th>c_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>b_1</td>
<td>2</td>
<td>9 - s</td>
<td>10 - t</td>
</tr>
<tr>
<td>b_2</td>
<td>s</td>
<td>t</td>
<td>3</td>
</tr>
</tbody>
</table>

In other words, \( f(x) = 3x^2 + 11x + 6 = (3x + 2)(x + 3) \).

Similarly, if \( f(x) = 2x^3 + 9x^2 + 10x + 3 \), then the corresponding factor puzzle is

<table>
<thead>
<tr>
<th>\times</th>
<th>c_1</th>
<th>c_2</th>
<th>c_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>b_1</td>
<td>2</td>
<td>9 - s</td>
<td>10 - t</td>
</tr>
<tr>
<td>b_2</td>
<td>s</td>
<td>t</td>
<td>3</td>
</tr>
</tbody>
</table>

By Theorem 2.2, this factor puzzle is solvable if \( s(9-x) = 2t \) and \( s(10-t) = 6 \), or \((s, t) = (1, 4), (2, 7), (6, 9)\). Hence, we have the following three solutions depicted in (P):

<table>
<thead>
<tr>
<th>\times</th>
<th>c_1</th>
<th>c_2</th>
<th>c_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>b_1</td>
<td>2</td>
<td>9 - s</td>
<td>10 - t</td>
</tr>
<tr>
<td>b_2</td>
<td>s</td>
<td>t</td>
<td>3</td>
</tr>
</tbody>
</table>

In other words, \( f(x) = 2x^3 + 9x^2 + 10x + 3 = (2x + 1)(x^2 + 4x + 3) = (x + 1)(2x^2 + 7x + 3) = (x + 3)(2x^2 + 3x + 1) \).

### 3. Factor puzzles and matrix factorization

Another perspective of factor puzzles is matrix factorization (Q):

\[
\begin{pmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}
= \begin{pmatrix}
  b_1 \\
  b_2 \\
  \vdots \\
  b_m
\end{pmatrix}
\begin{pmatrix}
  c_1 & c_2 & \cdots & c_n
\end{pmatrix}
\]

Note that matrices \( B \) and \( C \) constitute a factorization of the matrix \( A \).

That being said, an interesting observation is that if a square matrix \( A \) is factorizable in the fashion depicted above (Q), then the matrix is singular, i.e., \( \text{det}(A) = 0 \). This fact follows from the definition of determinant and Theorem 2.2. In particular, a \( 2 \times 2 \) matrix \( A \) is factorizable in the fashion depicted above (Q) if and only if the matrix is singular, i.e., \( \text{det}(A) = 0 \).
4. Use case

To secure communicating information, a sender encrypts the original message using a scheme (key), unknown except for the intended parties, and the intended receiver decrypts using the key inverse. One approach for encryption is to replace a text message by a sequence of numbers using a linear transformation. Table 2 demonstrates a correspondence between English alphabets and the numbers $1 \rightarrow 26$. The space corresponds to number 27. Alternative correspondences are possible.

For example, consider the message “TOP SECURITY CLEARANCE”. Using the above tabulated correspondence (Table 2), this message can be written as follows:

<table>
<thead>
<tr>
<th>T</th>
<th>O</th>
<th>P</th>
<th>S</th>
<th>E</th>
<th>U</th>
<th>R</th>
<th>T</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>15</td>
<td>16</td>
<td>5</td>
<td>19</td>
<td>3</td>
<td>18</td>
<td>20</td>
<td>27</td>
</tr>
</tbody>
</table>

To encode the message, one can use, for example, the solution vectors of the following factor puzzle (R):

\[
\begin{bmatrix}
20 \\
15 \\
16 \\
5 \\
19 \\
3 \\
18 \\
20 \\
27 \\
\end{bmatrix}
\]

Consequently, the encrypted message, which will be sent along with the factor puzzle, will be as follows:

85 50 113 70 53 29 69 45 63 36 115 70 63 33 55 30 56 37 29 44 29 21 13.

The calculations are explained below (S).

To decode the received message, the receiver can solve the factor puzzle and then use the inverse matrix for decryption.

Note that the solution is unique in this.

5. Conclusion

In this paper, we defined factor puzzles and their solutions. Furthermore, we addressed the important questions of existence and uniqueness of solutions, number of solutions, and its connections to polynomial and matrix factorizations. In addition, application to cryptography was discussed.

While the factor puzzles might be elementary, the combination of ideas presented in this manuscript are far from being elementary. Furthermore, while this line of research is still in its infancy, there is ample room for extension.
Data availability
There is no data associated with this article.

References


The benefits of publishing with F1000Research:

• Your article is published within days, with no editorial bias
• You can publish traditional articles, null/negative results, case reports, data notes and more
• The peer review process is transparent and collaborative
• Your article is indexed in PubMed after passing peer review
• Dedicated customer support at every stage

For pre-submission enquiries, contact research@f1000.com