Gaussian Elimination over $\text{GF}(2)$
Finding Perfect Squares

- Integer factorization algorithms triangularization of a Boolean matrix
- The operations are performed in the Galois field of 2 elements
- This stems from the following problem:

**Problem Statement**

Given a set of positive integers \( \{Q_1, Q_2, \ldots, Q_n\} \), find a subset \( R \subset Q \) such that the product of all \( Q_i \in R \) is a perfect square.

To find \( R \), first factor each \( Q_i \) into a factor base, i.e., a set of predetermined prime numbers \( \{p_1, p_2, \ldots, p_m\} \)

\[
Q_i = p_1^{a_{i1}} \cdot p_2^{a_{i2}} \cdots p_m^{a_{im}}
\]

for all \( i = 1, 2, \ldots, n \)
The Method

Now consider the $n \times m$ matrix

$$A = [A_{ij}] = [a_{ij} \pmod{2}]$$

with entries consisting from $\{0, 1\}$ for $1 \leq i \leq n$ and $1 \leq j \leq m$

We apply *elementary column operations* to this matrix in the field GF(2), and mark each row in which a pivot element is located.

An unmarked nonzero row at the end of the elimination process implies the existence of a subset $R$ satisfying the perfect square property.
An Example

- Consider $Q = \{6, 42, 105, 20, 63\}$ with the factor base $P = \{2, 3, 5, 7\}$
- We expand the elements of $Q$ into the factor base as

$$
\begin{align*}
6 &= 2^1 3^1 5^0 7^0 \\
42 &= 2^1 3^1 5^0 7^1 \\
105 &= 2^0 3^1 5^1 7^1 \\
20 &= 2^2 3^0 5^1 7^0 \\
63 &= 2^0 3^2 5^0 7^1
\end{align*}
$$

- This gives $A$ as

\[
A = \begin{bmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 \\
2 & 0 & 1 & 0 \\
0 & 2 & 0 & 1
\end{bmatrix} \pmod{2} = \begin{bmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
First Pivot

- On this matrix we perform elementary column operations and mark each row on which we find a pivot.
- We start with the first column, and search for a pivot in this column.
- Since $A_{11} = 1$, it is selected as the pivot element and column 1 as the pivot column.

$$
\begin{bmatrix}
1 & 1 & 0 & 0 & * \\
1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
$$
First Pivot

- We then perform a search for 1s in the row in which the pivot element is found.
- If element $A_{1k} = 1$ for $k \neq 1$ is nonzero, we add column 1 to column $k$ in GF(2).
- Since $A_{12} = 1$, we add column 1 to column 2 to obtain the updated column 2:

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & * \\
1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 
\end{bmatrix}
$$
Second Pivot

- We then proceed to pick column 2 and search for a pivot in this column.
- Since $A_{32} = 1$, we mark row 3, and search for 1s in row 3.

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & \star \\
1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & \star \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
$$
We find $A_{33} = A_{34} = 1$, thus add column 2 to columns 3 and 4:

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & \star \\
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & \star \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
Third Pivot

- The next pivot is $A_{43}$
- However, there are no other 1s in row 4
- We only mark row 4 and obtain:

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & * \\
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & * \\
0 & 0 & 1 & 0 & * \\
0 & 0 & 0 & 1
\end{bmatrix}
$$
Fourth Pivot

- The last pivot found is $A_{24}$

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & \star \\
1 & 0 & 0 & 1 & \star \\
0 & 1 & 0 & 0 & \star \\
0 & 0 & 1 & 0 & \star \\
0 & 0 & 0 & 1 & \\
\end{bmatrix}
\]

- Since $A_{21} = 1$, we add column 4 to column 1, and obtain

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & \star \\
0 & 0 & 0 & 1 & \star \\
0 & 1 & 0 & 0 & \star \\
0 & 0 & 1 & 0 & \star \\
1 & 0 & 0 & 1 & \\
\end{bmatrix}
\]
Next Step

- Since we are done with finding and marking pivots, we look for an unmarked row which indicates the existence of a subset \( R \).
- The row 5 has not been used.
- Since \( A_{51} = A_{54} = 1 \), row 5 and all rows \( i \) for which \( A_{i1} = 1 \) or \( A_{i4} = 1 \) are dependent.

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & \leftarrow \\
0 & 0 & 0 & 1 & \leftarrow \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & \leftarrow
\end{bmatrix}
\]

- From the matrix we see that rows 1, 2, and 5 are dependent.
If we sum row 1, row 2, and row 5 in GF(2), we obtain a zero row:

\[
\begin{align*}
1000 & \quad \text{Row 1} \quad Q_1 = 6 \\
0001 & \quad \text{Row 2} \quad Q_2 = 42 \\
1001 & \quad \text{Row 5} \quad Q_5 = 63 \\
\oplus & \quad 0000
\end{align*}
\]
Finding the Subset $R$

This implies that $R = \{Q_1, Q_2, Q_5\}$ and the product $Q_1 \cdot Q_2 \cdot Q_5$ forms a perfect square:

\[
Q_1 Q_2 Q_5 = 6 \cdot 42 \cdot 63
\]

\[
= (2^1 3^1 5^0 7^0)(2^1 3^1 5^0 7^1)(2^0 3^2 5^0 7^1)
\]

\[
= 2^2 3^4 5^0 7^2
\]

\[
= (2^1 3^2 5^0 7^1)^2
\]

\[
= 126^2
\]
The Algorithm

for $j = 1, 2, \ldots, m$
   Search for $A_{ij} = 1$ in Column $j$
   if found then
      Mark row $i$
      for $k = 1, 2, \ldots, j - 1, j + 1, \ldots, m$
         if $A_{ik} = 1$ then add column $j$ to column $k$

Theorem

*The sequential Gaussian elimination algorithm requires* $m^2n + m^2 - m$ *GF(2) operations to triangularize an* $n \times m$ *matrix.*
References


