Factorization and Primality Testing Chapter 8 The Quadratic Sieve

Robert C. Vaughan

November 4, 2024

Prolegomenon

- There have been many factorization algorithms developed with the intent of finding t, x, y so that

$$tn = x^2 - y^2, \tag{1.1}$$

Prolegomenon

- There have been many factorization algorithms developed with the intent of finding t, x, y so that

$$tn = x^2 - y^2, \tag{1.1}$$

- going back to Fermat in the case $t = 1$ and Legendre for general t.

Prolegomenon

- There have been many factorization algorithms developed with the intent of finding t, x, y so that

$$tn = x^2 - y^2, \tag{1.1}$$

- going back to Fermat in the case $t = 1$ and Legendre for general t.
- One of the lines of attack was through the use of continued fractions.

Prolegomenon

- There have been many factorization algorithms developed with the intent of finding t, x, y so that

$$tn = x^2 - y^2, \tag{1.1}$$

- going back to Fermat in the case $t = 1$ and Legendre for general t.
- One of the lines of attack was through the use of continued fractions.
- It seems to have been periodically rediscovered, for example by Kraitchik and, most notably, by Lehmer and Powers in 1931 and then developed further by Morrison and Brillhart in 1975 who showed that the advent of modern computers made it a practical method.

- The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- This expansion is actually periodic, and truncating the expansion after k terms produces an approximation

$$\frac{A_k}{B_k} \tag{1.2}$$

to $\sqrt{tn}$.

- The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- This expansion is actually periodic, and truncating the expansion after k terms produces an approximation

$$\frac{A_k}{B_k} \tag{1.2}$$

to $\sqrt{tn}$.

- In particular

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k \tag{1.3}$$

where R_k is relatively small.

- The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- This expansion is actually periodic, and truncating the expansion after k terms produces an approximation

$$\frac{A_k}{B_k} \tag{1.2}$$

to $\sqrt{tn}$.

- In particular

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k \tag{1.3}$$

where R_k is relatively small.

- By the way the approximation (1.2) turns out to be exactly the approximation that would arise from an application of Dirichlet's theorem, Theorem 2.2.

- The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

- This expansion is actually periodic, and truncating the expansion after k terms produces an approximation

$$\frac{A_k}{B_k} \tag{1.2}$$

to $\sqrt{tn}$.

- In particular

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k \tag{1.3}$$

where R_k is relatively small.

- By the way the approximation (1.2) turns out to be exactly the approximation that would arise from an application of Dirichlet's theorem, Theorem 2.2.
- Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1}R_k \pmod{n}.$$

- Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1} R_k \pmod{n}.$$

- Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1} R_k \pmod{n}.$$

- Having computed $(-1)^{k-1}R_k$ for $k = 0, \ldots K$ one looks for a subset $\mathcal{K}$ of the k such that the product

$$\prod_{k \in \mathcal{K}} (-1)^{k-1} R_k$$

is a perfect square.

- Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1} R_k \pmod n.$$

- Having computed $(-1)^{k-1} R_k$ for $k = 0, \ldots K$ one looks for a subset $\mathcal{K}$ of the k such that the product

$$\prod_{k \in \mathcal{K}} (-1)^{k-1} R_k$$

is a perfect square.

- Then for

$$R \equiv \prod_{k \in \mathcal{K}} (-1)^{k-1} R_k \pmod n, \; A \equiv \prod_{k \in \mathcal{K}} A_k \pmod n$$

one has

$$A^2 \equiv R^2 \pmod n$$

- Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1} R_k \pmod{n}.$$

- Having computed $(-1)^{k-1} R_k$ for $k = 0, \ldots K$ one looks for a subset $\mathcal{K}$ of the k such that the product

$$\prod_{k \in \mathcal{K}} (-1)^{k-1} R_k$$

is a perfect square.

- Then for

$$R \equiv \prod_{k \in \mathcal{K}} (-1)^{k-1} R_k \pmod{n}, \; A \equiv \prod_{k \in \mathcal{K}} A_k \pmod{n}$$

one has

$$A^2 \equiv R^2 \pmod{n}$$

- and hopefully $GCD(A \pm R, n)$ provides a proper factor of n.

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).
- The expression in (1.3) on the left

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k$$

can be thought of as an indefinite binary quadratic form

$$x^2 - tny^2.$$

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).
- The expression in (1.3) on the left

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k$$

can be thought of as an indefinite binary quadratic form

$$x^2 - tny^2.$$

- Gauss had already studied such forms and had introduced the idea of “composition” of forms.

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).
- The expression in (1.3) on the left
$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k$$
can be thought of as an indefinite binary quadratic form
$$x^2 - tny^2.$$
- Gauss had already studied such forms and had introduced the idea of "composition" of forms.
- This lead Shanks to bring such structural ideas to the party, and gave arise to an alternative version of the method usually known as SQUFOF.

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).
- The expression in (1.3) on the left

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k$$

can be thought of as an indefinite binary quadratic form

$$x^2 - tny^2.$$

- Gauss had already studied such forms and had introduced the idea of "composition" of forms.
- This lead Shanks to bring such structural ideas to the party, and gave arise to an alternative version of the method usually known as SQUFOF.
- This has a worse case runtime proportional to $n^{1/4}$, so does not compete in that regard to the other methods described here.

- Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).
- The expression in (1.3) on the left
$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k$$
can be thought of as an indefinite binary quadratic form
$$x^2 - tny^2.$$
- Gauss had already studied such forms and had introduced the idea of “composition” of forms.
- This lead Shanks to bring such structural ideas to the party, and gave arise to an alternative version of the method usually known as SQUFOF.
- This has a worse case runtime proportional to $n^{1/4}$, so does not compete in that regard to the other methods described here.
- However SQUFOF (SQUareFOrmsFactorization) is sufficiently simple that it can be implemented on a pocket calculator and the instructor of this course has a version on his mobile phone.

The Quadratic Sieve

- Recall that in Lehman's method the aim is to find x, t so that

$$x^2 - 4tn$$

is a perfect square.

The Quadratic Sieve

- Recall that in Lehman's method the aim is to find x, t so that
$$x^2 - 4tn$$
is a perfect square.
- In the discussion above of the continued fraction approach we saw that an alternative way to achieve this is to find $x_1, \ldots, x_r$ and $y_1, \ldots, y_r$ such that
$$y_i \equiv x_i^2 \pmod{n}$$
and
$$(x_1 \ldots x_r)^2 \equiv y_1 \ldots y_r = z^2 \pmod{n}.$$

The Quadratic Sieve

- Recall that in Lehman's method the aim is to find x, t so that
$$x^2 - 4tn$$
is a perfect square.
- In the discussion above of the continued fraction approach we saw that an alternative way to achieve this is to find $x_1, \ldots, x_r$ and $y_1, \ldots, y_r$ such that
$$y_i \equiv x_i^2 \pmod{n}$$
and
$$(x_1 \ldots x_r)^2 \equiv y_1 \ldots y_r = z^2 \pmod{n}.$$
- However we want something better than trial and error.

The Quadratic Sieve

- **Idea.** Initially we consider

$$x^2 - n = y$$

with for a sequence of values of $x = x_j$.

The Quadratic Sieve

- **Idea.** Initially we consider
$$x^2 - n = y$$
with for a sequence of values of $x = x_j$.
- The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square.

The Quadratic Sieve

- **Idea.** Initially we consider
$$x^2 - n = y$$
with for a sequence of values of $x = x_j$.
- The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square.
- Suppose that each of the y_j has only small prime factors, say we have $p \le B$ for every $p | y_j$.

The Quadratic Sieve

- **Idea.** Initially we consider
$$x^2 - n = y$$
with for a sequence of values of $x = x_j$.
- The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square.
- Suppose that each of the y_j has only small prime factors, say we have $p \le B$ for every $p|y_j$.
- For example we just look for prime factors $p \le B = 7$ and suppose we found $y_1 = 6, y_2 = 15, y_3 = 21, y_4 = 35$.

The Quadratic Sieve

- **Idea.** Initially we consider
$$x^2 - n = y$$
with for a sequence of values of $x = x_j$.
- The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square.
- Suppose that each of the y_j has only small prime factors, say we have $p \le B$ for every $p | y_j$.
- For example we just look for prime factors $p \le B = 7$ and suppose we found $y_1 = 6, y_2 = 15, y_3 = 21, y_4 = 35$.
- Then we would have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$

The Quadratic Sieve

- **Idea.** Initially we consider
$$x^2 - n = y$$
with for a sequence of values of $x = x_j$.
- The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square.
- Suppose that each of the y_j has only small prime factors, say we have $p \le B$ for every $p|y_j$.
- For example we just look for prime factors $p \le B = 7$ and suppose we found $y_1 = 6, y_2 = 15, y_3 = 21, y_4 = 35$.
- Then we would have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$
- so we can associate with these the four vectors
$$\mathbf{v}_1 = \langle 1, 1, 0, 0 \rangle, \mathbf{v}_2 = \langle 0, 1, 1, 0 \rangle,$$
$$\mathbf{v}_3 = \langle 0, 1, 0, 1 \rangle, \mathbf{v}_4 = \langle 0, 0, 1, 1 \rangle.$$

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,

$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$
- so we can associate with these the four vectors
$$\mathbf{v}_1 = \langle 1, 1, 0, 0 \rangle, \mathbf{v}_2 = \langle 0, 1, 1, 0 \rangle,$$
$$\mathbf{v}_3 = \langle 0, 1, 0, 1 \rangle, \mathbf{v}_4 = \langle 0, 0, 1, 1 \rangle.$$

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$
- so we can associate with these the four vectors
$$\mathbf{v}_1 = \langle 1,1,0,0\rangle, \mathbf{v}_2 = \langle 0,1,1,0\rangle,$$
$$\mathbf{v}_3 = \langle 0,1,0,1\rangle, \mathbf{v}_4 = \langle 0,0,1,1\rangle.$$
- Then we want to find integers $e_j = 0$ or 1 so that
$$e_1\mathbf{v}_1 + e_2\mathbf{v}_2 + e_3\mathbf{v}_3 + e_4\mathbf{v}_4 \equiv \mathbf{0} \pmod 2$$
where $\mathbf{0} = \langle 0,0,0,0\rangle$.

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,

$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$

- so we can associate with these the four vectors

$$\mathbf{v}_1 = \langle 1,1,0,0\rangle, \mathbf{v}_2 = \langle 0,1,1,0\rangle,$$
$$\mathbf{v}_3 = \langle 0,1,0,1\rangle, \mathbf{v}_4 = \langle 0,0,1,1\rangle.$$

- Then we want to find integers $e_j = 0$ or 1 so that

$$e_1\mathbf{v}_1 + e_2\mathbf{v}_2 + e_3\mathbf{v}_3 + e_4\mathbf{v}_4 \equiv \mathbf{0} \pmod 2$$

  where $\mathbf{0} = \langle 0,0,0,0\rangle$.
- Thus $e_1 = 0$, $e_2 = e_3 = e_4 = 1$ will do and

$$y_1^0 y_2^1 y_3^1 y_4^1 = 15.21.35 = (3.5.7)^2 = (105)^2.$$

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$
- so we can associate with these the four vectors
$$\mathbf{v}_1 = \langle 1,1,0,0\rangle, \mathbf{v}_2 = \langle 0,1,1,0\rangle,$$
$$\mathbf{v}_3 = \langle 0,1,0,1\rangle, \mathbf{v}_4 = \langle 0,0,1,1\rangle.$$
- Then we want to find integers $e_j = 0$ or 1 so that
$$e_1\mathbf{v}_1 + e_2\mathbf{v}_2 + e_3\mathbf{v}_3 + e_4\mathbf{v}_4 \equiv \mathbf{0} \pmod 2$$
where $\mathbf{0} = \langle 0,0,0,0\rangle$.
- Thus $e_1 = 0$, $e_2 = e_3 = e_4 = 1$ will do and
$$y_1^0 y_2^1 y_3^1 y_4^1 = 15.21.35 = (3.5.7)^2 = (105)^2.$$
- Thus we can find perfect squares by vector addition. In other words solving linear equations.

The Quadratic Sieve

- We have $y_1 = 2^1 3^1 5^0 7^0$,
$$y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$
- so we can associate with these the four vectors
$$\mathbf{v}_1 = \langle 1,1,0,0\rangle, \mathbf{v}_2 = \langle 0,1,1,0\rangle,$$
$$\mathbf{v}_3 = \langle 0,1,0,1\rangle, \mathbf{v}_4 = \langle 0,0,1,1\rangle.$$
- Then we want to find integers $e_j = 0$ or 1 so that
$$e_1\mathbf{v}_1 + e_2\mathbf{v}_2 + e_3\mathbf{v}_3 + e_4\mathbf{v}_4 \equiv \mathbf{0} \pmod 2$$
where $\mathbf{0} = \langle 0,0,0,0\rangle$.
- Thus $e_1 = 0$, $e_2 = e_3 = e_4 = 1$ will do and
$$y_1^0 y_2^1 y_3^1 y_4^1 = 15.21.35 = (3.5.7)^2 = (105)^2.$$
- Thus we can find perfect squares by vector addition. In other words solving linear equations.
- In practice this in turn means Gaussian elimination.

The Quadratic Sieve

Definition 1

Given a positive real number B we say that an integer z is B-factorable when every prime factor p of z satisfies $p \le B$. To emphasise the fact that in our situation only certain primes (but also -1) may occur we will also use the term $\mathcal{P}$-factorable where $\mathcal{P}$ is a set of primes, probably augmented by -1.

- Note that the term B-smooth is commonly used instead. The word "smooth" has many better uses in mathematics.

- **The Quadratic Sieve (QS)**
  We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n.

- **The Quadratic Sieve (QS)**
  We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n.
- **1. Initialization.**
  1.1. *Pick a number B as the upper bound for the primes in the factor base $\mathcal{P}$. Theory says take $B = \lceil L(n)^{1/2} \rceil$ where $L(n) = \exp(\sqrt{\log n \log\log n})$, but in practice a B somewhat smaller works well.*

- **The Quadratic Sieve (QS)**
  We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n.
- **1. Initialization.**
  1.1. *Pick a number B as the upper bound for the primes in the factor base $\mathcal{P}$. Theory says take $B = \lceil L(n)^{1/2} \rceil$ where $L(n) = \exp(\sqrt{\log n \log\log n})$, but in practice a B somewhat smaller works well.*
- *Also, adding extra primes suggested by the sieving process can be useful and if one uses the wrinkle in 5.3 below, then the prime p is adjoined to the factor base.*

- **The Quadratic Sieve (QS)**
  We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n.
- **1. Initialization.**
  1.1. *Pick a number B as the upper bound for the primes in the factor base $\mathcal{P}$. Theory says take $B = \lceil L(n)^{1/2} \rceil$ where $L(n) = \exp(\sqrt{\log n \log\log n})$, but in practice a B somewhat smaller works well.*
- *Also, adding extra primes suggested by the sieving process can be useful and if one uses the wrinkle in 5.3 below, then the prime p is adjoined to the factor base.*
- **1.2.** *Set $p_0 = -1$, $p_1 = 2$ and find the odd primes $p_2 < p_3 < \ldots < p_K \leq B$ such that $\left(\frac{n}{p_k}\right)_L = 1$.*
- **(LJ)** *is useful here.*

- **The Quadratic Sieve (QS)**
We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n.
- **1. Initialization.**
1.1. *Pick a number B as the upper bound for the primes in the factor base $\mathcal{P}$. Theory says take $B = \lceil L(n)^{1/2} \rceil$ where $L(n) = \exp(\sqrt{\log n \log\log n})$, but in practice a B somewhat smaller works well.*
- *Also, adding extra primes suggested by the sieving process can be useful and if one uses the wrinkle in 5.3 below, then the prime p is adjoined to the factor base.*
- **1.2.** *Set $p_0 = -1$, $p_1 = 2$ and find the odd primes $p_2 < p_3 < \ldots < p_K \le B$ such that $\left(\frac{n}{p_k}\right)_L = 1$.*
- **(LJ)** *is useful here.*
- **1.3.** *For $k = 2, \ldots, K$ find the solutions $\pm t_{p_k}$ to $x^2 \equiv n \pmod{p_k}$ by using* **(QC)**.

- **2. Sieving.**
  2.1. Let $N = \lceil \sqrt{n} \rceil$. Sieve the sequence $x^2 - n$ with $x = N + j$, $j = 0, \pm 1, \pm 2, \ldots$ until one has obtained a list of at least $K + 2$ B-factorable $x_j^2 - n$ and their factorizations ($K + 2$ is somewhat arbitrary and in the first example below is $K + 1$).

- **2. Sieving.**
  2.1. Let $N = \lceil \sqrt{n} \rceil$. Sieve the sequence $x^2 - n$ with $x = N + j$, $j = 0, \pm 1, \pm 2, \ldots$ until one has obtained a list of at least $K + 2$ B-factorable $x_j^2 - n$ and their factorizations ($K + 2$ is somewhat arbitrary and in the first example below is $K + 1$).
- *This could be done by using a matrix, with $K + 2$ rows so that the j–th column is a $K + 3$ dimensional vector in which the first entry is x_j, the second is $x_j^2 - n$, and the $k + 3$–rd entry is the exponent of p_k in $x_j^2 - n$.*

- **2. Sieving.**
  2.1. Let $N=\lceil\sqrt{n}\rceil$. Sieve the sequence x^2-n with $x=N+j$, $j=0,\pm1,\pm2,\ldots$ until one has obtained a list of at least $K+2$ B-factorable x_j^2-n and their factorizations ($K+2$ is somewhat arbitrary and in the first example below is $K+1$).
- *This could be done by using a matrix, with $K+2$ rows so that the j–th column is a $K+3$ dimensional vector in which the first entry is x_j, the second is x_j^2-n, and the $k+3$–rd entry is the exponent of p_k in x_j^2-n.*
- **2.2.** *For each prime p_k in $\mathcal{P}$ divide out all the prime factors p_k in each entry x_j^2-n with $x_j\equiv\pm t_{p_k} \pmod{p_k}$, recording the exponent in the $k+3$-rd entry in the associated j-th vector. Once the primes start to grow this speeds things up significantly.*

- **2. Sieving.**
  2.1. Let $N = \lceil \sqrt{n} \rceil$. Sieve the sequence $x^2 - n$ with $x = N + j$, $j = 0, \pm 1, \pm 2, \ldots$ until one has obtained a list of at least $K + 2$ B-factorable $x_j^2 - n$ and their factorizations ($K + 2$ is somewhat arbitrary and in the first example below is $K + 1$).
- *This could be done by using a matrix, with $K + 2$ rows so that the j–th column is a $K + 3$ dimensional vector in which the first entry is x_j, the second is $x_j^2 - n$, and the $k + 3$–rd entry is the exponent of p_k in $x_j^2 - n$.*
- **2.2.** *For each prime p_k in $\mathcal{P}$ divide out all the prime factors p_k in each entry $x_j^2 - n$ with $x_j \equiv \pm t_{p_k} \pmod{p_k}$, recording the exponent in the $k + 3$-rd entry in the associated j-th vector. Once the primes start to grow this speeds things up significantly.*
- **2.3.** *If the bottom entry in the j–th vector has reduced to 1, then $x_j^2 - n$ is B–factorable. If it has not completely factored then one can discard that column, or at least put it aside in case one needs to extend the factor base.*

- **3. Linear Algebra.**
  3.1. *Form a* $(K+1)\times(K+2)$ *matrix* $\mathcal{M}$ *with the columns being formed by the* 3–*rd through* $K+3$–*rd entries of the column vectors arising in* **2.2**, *but with the entries reduced modulo* 2.

- **3. Linear Algebra.**
  3.1. *Form a* $(K+1) \times (K+2)$ *matrix* $\mathcal{M}$ *with the columns being formed by the* 3–*rd through* $K+3$–*rd entries of the column vectors arising in* **2.2**, *but with the entries reduced modulo* 2.
- **3.2.** *Use linear algebra (Gaussian elimination, for example) to solve*

$$\mathcal{M}\mathbf{e} = \mathbf{0} \pmod 2$$

where $\mathbf{e}$ *is a* $K+2$ *dimensional vector of* 0*s and* 1*s (not all* 0*!).*

- **3. Linear Algebra.**
  3.1. *Form a* $(K+1)\times(K+2)$ *matrix* $\mathcal{M}$ *with the columns being formed by the* 3–rd *through* $K+3$–rd *entries of the column vectors arising in* **2.2**, *but with the entries reduced modulo* 2.
- **3.2.** *Use linear algebra (Gaussian elimination, for example) to solve*

$$\mathcal{M}\mathbf{e}=\mathbf{0}\pmod 2$$

where $\mathbf{e}$ *is a* $K+2$ *dimensional vector of* 0*s and* 1*s (not all* 0*!).*
- *Note that the solution space may well be of dimension greater than* 1 *so then there would be multiple solutions.*

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

modulo n.

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1} (x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

  modulo n.
- *The value of* x *can be computed by using the first entries in the* j*–vectors.*

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

  modulo n*.*
- *The value of* x *can be computed by using the first entries in the* j*–vectors.*
- *The square root should NOT be computed directly but by using the factorisations of each* $x_j^2 - n$ *obtained in* **2.2***.*

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

  modulo n.
- *The value of* x *can be computed by using the first entries in the* j*–vectors.*
- *The square root should NOT be computed directly but by using the factorisations of each* $x_j^2 - n$ *obtained in* **2.2**.
- **4.2.** *Compute* $m = \gcd(x - y, n)$.

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

  modulo n.
- *The value of* x *can be computed by using the first entries in the* j*–vectors.*
- *The square root should NOT be computed directly but by using the factorisations of each* $x_j^2 - n$ *obtained in* **2.2**.
- **4.2.** *Compute* $m = \gcd(x - y, n)$.
- **4.3.** *Return* m.

- **4. Factorization.**
  4.1. *Compute* $x = x_1^{e_1} x_2^{e_2} \dots x_{K+2}^{e_{K+2}}$ *modulo* n *and*

$$y = \sqrt{(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \dots (x_{K+2}^2 - n)^{e_{K+2}}}$$

  modulo n*.*
- *The value of* x *can be computed by using the first entries in the* j*–vectors.*
- *The square root should NOT be computed directly but by using the factorisations of each* $x_j^2 - n$ *obtained in* **2.2***.*
- **4.2.** *Compute* $m = \gcd(x - y, n)$*.*
- **4.3.** *Return* m*.*
- **4.4.** *If necessary repeat for all solutions* **e** *until a non-trivial factor found.*

- **5. Aftermath.**
  5.1. *If no proper factor of n found, try one or more of the following.*

- **5. Aftermath.**
  5.1. *If no proper factor of* n *found, try one or more of the following.*
- **5.2.** *Extend the sieving in 2.1 to obtain more* $\mathbf{e}$ *and pairs* x, y.

- **5. Aftermath.**
  5.1. *If no proper factor of n found, try one or more of the following.*
- **5.2.** *Extend the sieving in 2.1 to obtain more* **e** *and pairs x, y.*
- **5.3** *As a matter of policy the original sieving probably should be conducted so as to obtain K' pairs with K' somewhat more than $K+2$.*

- **5. Aftermath.**
  5.1. *If no proper factor of n found, try one or more of the following.*
- **5.2.** *Extend the sieving in 2.1 to obtain more* $\mathbf{e}$ *and pairs* x, y.
- **5.3** *As a matter of policy the original sieving probably should be conducted so as to obtain K' pairs with K' somewhat more than $K+2$.*
- **5.3.** *Use another polynomial in place of $x^2 - n$, or rather, be a bit more cunning about the choice of the x in 2.1. Choose a large prime p for which $b^2 - n \equiv 0 \pmod{p}$ is soluble, and compute b. Then $(px+b)^2 - n \equiv 0 \pmod{p}$ and x can be chosen so that $f(x) = ((px+b)^2 - n)/p$ is comparatively small since p is large, so the sieving proceeds relatively speedily, there is a better chance of a complete factorization of $f(x)$, and we only have to augment the factor base with the prime p.*

- The most time consuming part of this algorithm is the sieving.

- The most time consuming part of this algorithm is the sieving.
- Note that just restricting the x to $x \equiv \pm t_{p_k}$ already speeds it up considerably but this is still usually the slowest part.

- The most time consuming part of this algorithm is the sieving.
- Note that just restricting the x to $x \equiv \pm t_{p_k}$ already speeds it up considerably but this is still usually the slowest part.
- The linear algebra can also be speeded up by various techniques, especially those developed for dealing with sparse matrices.

- The most time consuming part of this algorithm is the sieving.
- Note that just restricting the x to $x \equiv \pm t_{p_k}$ already speeds it up considerably but this is still usually the slowest part.
- The linear algebra can also be speeded up by various techniques, especially those developed for dealing with sparse matrices.
- Although the numbers in the following example are much smaller than would occur in a practice the example does illustrate the complexity of the basic quadratic sieve.

- **Example 8.1.** *Let* $n = 9487$ *and* $B = 30$.

- **Example 8.1.** *Let* $n = 9487$ *and* $B = 30$*.*
- We first need to check which primes $p \le 30$ will occur.

- **Example 8.1.** *Let* $n = 9487$ *and* $B = 30$.
- We first need to check which primes $p \le 30$ will occur.
- Thus for each odd prime $p \le 30$ we need to ascertain whether n is a QR or a QNR modulo p.

$$\left(\frac{9487}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1, \left(\frac{9487}{13}\right)_L = \left(\frac{10}{13}\right)_L = \left(\frac{36}{13}\right)_L = 1,$$
$$\left(\frac{9487}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1, \left(\frac{9487}{17}\right)_L = \left(\frac{1}{17}\right) = 1,$$
$$\left(\frac{9487}{7}\right)_L = \left(\frac{2}{7}\right)_L = 1, \left(\frac{9487}{19}\right)_L = \left(\frac{6}{19}\right)_L = \left(\frac{25}{19}\right)_L = 1,$$
$$\left(\frac{9487}{11}\right)_L = \left(\frac{5}{11}\right)_L = 1, \left(\frac{9487}{23}\right)_L = \left(\frac{11}{23}\right)_L = -\left(\frac{23}{11}\right)_L = -1,$$
$$\left(\frac{9487}{29}\right)_L = \left(\frac{4}{29}\right)_L = 1.$$

- **Example 8.1.** *Let* $n = 9487$ *and* $B = 30$*.*
- We first need to check which primes $p \le 30$ will occur.
- Thus for each odd prime $p \le 30$ we need to ascertain whether n is a QR or a QNR modulo p.

$$\left(\frac{9487}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1, \left(\frac{9487}{13}\right)_L = \left(\frac{10}{13}\right)_L = \left(\frac{36}{13}\right)_L = 1,$$
$$\left(\frac{9487}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1, \left(\frac{9487}{17}\right)_L = \left(\frac{1}{17}\right) = 1,$$
$$\left(\frac{9487}{7}\right)_L = \left(\frac{2}{7}\right)_L = 1, \left(\frac{9487}{19}\right)_L = \left(\frac{6}{19}\right)_L = \left(\frac{25}{19}\right)_L = 1,$$
$$\left(\frac{9487}{11}\right)_L = \left(\frac{5}{11}\right)_L = 1, \left(\frac{9487}{23}\right)_L = \left(\frac{11}{23}\right)_L = -\left(\frac{23}{11}\right)_L = -1,$$
$$\left(\frac{9487}{29}\right)_L = \left(\frac{4}{29}\right)_L = 1.$$

- Thus $\mathcal{P} = \{-1, 2, 3, 7, 11, 13, 17, 19, 29\}$.

- **Example 8.1.** *Let* $n = 9487$ *and* $B = 30$.
- We first need to check which primes $p \le 30$ will occur.
- Thus for each odd prime $p \le 30$ we need to ascertain whether n is a QR or a QNR modulo p.

$$\left(\frac{9487}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1, \left(\frac{9487}{13}\right)_L = \left(\frac{10}{13}\right)_L = \left(\frac{36}{13}\right)_L = 1,$$
$$\left(\frac{9487}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1, \left(\frac{9487}{17}\right)_L = \left(\frac{1}{17}\right) = 1,$$
$$\left(\frac{9487}{7}\right)_L = \left(\frac{2}{7}\right)_L = 1, \left(\frac{9487}{19}\right)_L = \left(\frac{6}{19}\right)_L = \left(\frac{25}{19}\right)_L = 1,$$
$$\left(\frac{9487}{11}\right)_L = \left(\frac{5}{11}\right)_L = 1, \left(\frac{9487}{23}\right)_L = \left(\frac{11}{23}\right)_L = -\left(\frac{23}{11}\right)_L = -1,$$
$$\left(\frac{9487}{29}\right)_L = \left(\frac{4}{29}\right)_L = 1.$$

- Thus $\mathcal{P} = \{-1, 2, 3, 7, 11, 13, 17, 19, 29\}$.
- Then by bf (QC) $t_3 = \pm 1, t_7 = \pm 3, t_{11} = \pm 4,$

$$t_{13} = \pm 5, t_{17} = \pm 1, t_{19} = \pm 5, t_{29} = \pm 2.$$

- **Example 8.1.** *Let $n = 9487$ and $B = 30$.*
- We first need to check which primes $p \le 30$ will occur.
- Thus for each odd prime $p \le 30$ we need to ascertain whether n is a QR or a QNR modulo p.

$$\left(\frac{9487}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1, \left(\frac{9487}{13}\right)_L = \left(\frac{10}{13}\right)_L = \left(\frac{36}{13}\right)_L = 1,$$
$$\left(\frac{9487}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1, \left(\frac{9487}{17}\right)_L = \left(\frac{1}{17}\right) = 1,$$
$$\left(\frac{9487}{7}\right)_L = \left(\frac{2}{7}\right)_L = 1, \left(\frac{9487}{19}\right)_L = \left(\frac{6}{19}\right)_L = \left(\frac{25}{19}\right)_L = 1,$$
$$\left(\frac{9487}{11}\right)_L = \left(\frac{5}{11}\right)_L = 1, \left(\frac{9487}{23}\right)_L = \left(\frac{11}{23}\right)_L = -\left(\frac{23}{11}\right)_L = -1,$$
$$\left(\frac{9487}{29}\right)_L = \left(\frac{4}{29}\right)_L = 1.$$

- Thus $\mathcal{P} = \{-1, 2, 3, 7, 11, 13, 17, 19, 29\}$.
- Then by bf (QC) $t_3 = \pm 1, t_7 = \pm 3, t_{11} = \pm 4,$

$$t_{13} = \pm 5, t_{17} = \pm 1, t_{19} = \pm 5, t_{29} = \pm 2.$$

- Now for a range of values of x near $\sqrt{n} \approx 97$ we factorise $f(x) = x^2 - n$. At this stage we throw away the x which do not completely factor in our factor base.

- Show Class467-08T1.pdf.

- Show Class467-08T1.pdf.
- In the table above, in the column below each prime I have included the exponent of the prime which occurs in the factorisation and the residual factor after that prime has been factored out.

- I have included one such value, $x = 82$, below, so that you can see what happens. If n is proving awkward to factorise, one might go back and check to see if there are primes outside the factor base which occur in multiple places and then add them to the factor base. For example, $f(92)$ and $f(94)$ would completely factorise if we included the prime 31 in the factor base.

x	82	92	94
$f(x)$	-2763	-1023	-651
-1	2763,1	2763,0	651,1
2	2763,0	1023,1	651,0
3	307,2	341,1	217,1
7	307,0	341,0	31,1
11	307,0	31,0	31,0
13	307,0	31,0	31,0
17	307,0	31,0	31,0
19	307,0	31,0	31,0
29	307,0	31,0	31,0

- Let $\mathbf{v}(x)$ denote the vector of exponents in the factorization of $f(x)$, so that

$$\begin{aligned}\mathbf{v}(85) &= \langle 1,1,1,0,0,1,0,0,1\rangle,\\ \mathbf{v}(89) &= \langle 1,1,3,0,0,0,0,0,1\rangle,\\ \mathbf{v}(98) &= \langle 0,0,2,0,0,1,0,0,0\rangle,\end{aligned}$$

- Let $\mathbf{v}(x)$ denote the vector of exponents in the factorization of $f(x)$, so that

$$\mathbf{v}(85) = \langle 1, 1, 1, 0, 0, 1, 0, 0, 1\rangle,$$
$$\mathbf{v}(89) = \langle 1, 1, 3, 0, 0, 0, 0, 0, 1\rangle,$$
$$\mathbf{v}(98) = \langle 0, 0, 2, 0, 0, 1, 0, 0, 0\rangle,$$

- Then $\mathbf{v}(85) + \mathbf{v}(89) + \mathbf{v}(98) = \langle 2, 2, 6, 0, 0, 2, 0, 0, 2\rangle$ and the entries in this are all even.

- Let $\mathbf{v}(x)$ denote the vector of exponents in the factorization of $f(x)$, so that

$$\mathbf{v}(85) = \langle 1,1,1,0,0,1,0,0,1\rangle,$$
$$\mathbf{v}(89) = \langle 1,1,3,0,0,0,0,0,1\rangle,$$
$$\mathbf{v}(98) = \langle 0,0,2,0,0,1,0,0,0\rangle,$$

- Then $\mathbf{v}(85)+\mathbf{v}(89)+\mathbf{v}(98) = \langle 2,2,6,0,0,2,0,0,2\rangle$ and the entries in this are all even.
- Thus, modulo 9487,

$$\begin{aligned} 85^2 \times 89^2 \times 98^2 &\equiv (85^2-n)(89^2-n)(98^2-n) \\ 741370^2 &\equiv (-1\times 2\times 3^3\times 13\times 29)^2 = 20358^2. \end{aligned}$$

- Let $\mathbf{v}(x)$ denote the vector of exponents in the factorization of $f(x)$, so that

$$\begin{aligned}\mathbf{v}(85) &= \langle 1,1,1,0,0,1,0,0,1\rangle,\\ \mathbf{v}(89) &= \langle 1,1,3,0,0,0,0,0,1\rangle,\\ \mathbf{v}(98) &= \langle 0,0,2,0,0,1,0,0,0\rangle,\end{aligned}$$

- Then $\mathbf{v}(85)+\mathbf{v}(89)+\mathbf{v}(98) = \langle 2,2,6,0,0,2,0,0,2\rangle$ and the entries in this are all even.
- Thus, modulo 9487,

$$\begin{aligned}85^2 \times 89^2 \times 98^2 &\equiv (85^2-n)(89^2-n)(98^2-n)\\ 741370^2 &\equiv (-1\times 2\times 3^3\times 13\times 29)^2 = 20358^2.\end{aligned}$$

- Unfortunately

$$\begin{aligned}(741370+20358, 9487) &= 1,\\ (741370-20358, 9487) &= 9487.\end{aligned}$$

- We also have

$$\mathbf{v}(81) + \mathbf{v}(95) + \mathbf{v}(100) = \langle 2, 2, 4, 2, 2, 0, 0, 2, 0 \rangle,$$

- We also have

$$\mathbf{v}(81) + \mathbf{v}(95) + \mathbf{v}(100) = \langle 2, 2, 4, 2, 2, 0, 0, 2, 0 \rangle,$$

- so that

$$81^2 \times 95^2 \times 100^2 \equiv (-1 \times 2 \times 3^2 \times 7 \times 11 \times 19)^2 \pmod{9487}.$$

- We also have

$$\mathbf{v}(81) + \mathbf{v}(95) + \mathbf{v}(100) = \langle 2, 2, 4, 2, 2, 0, 0, 2, 0 \rangle,$$

- so that

$$81^2 \times 95^2 \times 100^2 \equiv (-1 \times 2 \times 3^2 \times 7 \times 11 \times 19)^2 \pmod{9487}.$$

- This gives

$$769500^2 \equiv 26334^2 \pmod{9487}$$

- We also have

$$\mathbf{v}(81)+\mathbf{v}(95)+\mathbf{v}(100)=\langle 2,2,4,2,2,0,0,2,0\rangle,$$

- so that

$$81^2\times 95^2\times 100^2\equiv(-1\times 2\times 3^2\times 7\times 11\times 19)^2 \pmod{9487}.$$

- This gives

$$769500^2\equiv 26334^2 \pmod{9487}$$

- and

$$(769500+26334,9487)=179,$$
$$(769500-26334,9487)=53.$$

- There is a lot to take away from this.

- There is a lot to take away from this.
- 1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.

- There is a lot to take away from this.
- 1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.
- 2. We then need to sieve out the x, i.e remove those x for which $f(x)$ does not completely factor in the factor base, and then to store the vector of exponents for each x which survives.

- There is a lot to take away from this.
- 1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.
- 2. We then need to sieve out the x, i.e remove those x for which $f(x)$ does not completely factor in the factor base, and then to store the vector of exponents for each x which survives.
- This can take a lot of memory.

- There is a lot to take away from this.
- 1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.
- 2. We then need to sieve out the x, i.e remove those x for which $f(x)$ does not completely factor in the factor base, and then to store the vector of exponents for each x which survives.
- This can take a lot of memory.
- 3. Whilst not apparent in the simple example above, we will need to work hard to find linear combinations of the vectors of exponents in which all the entries are even.

- There is a lot to take away from this.
- 1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.
- 2. We then need to sieve out the x, i.e remove those x for which $f(x)$ does not completely factor in the factor base, and then to store the vector of exponents for each x which survives.
- This can take a lot of memory.
- 3. Whilst not apparent in the simple example above, we will need to work hard to find linear combinations of the vectors of exponents in which all the entries are even.
- This will involve some form of Gaussian elimination. The complexity is somewhat reduced by the fact that we only need to do this modulo 2, but it will still also require quite a lot of memory.

- Going back to the table. Show Class467-08T1.pdf.

- Going back to the table. Show Class467-08T1.pdf.
- We can extract the exponents of each prime thus

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- Going back to the table. Show Class467-08T1.pdf.
- We can extract the exponents of each prime thus

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- Then we wish to find solutions to $\mathcal{M}\mathbf{e} \equiv \mathbf{0} \pmod{2}$ other than $\mathbf{0}$.

- Going back to the table. Show Class467-08T1.pdf.
- We can extract the exponents of each prime thus

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- Then we wish to find solutions to $\mathcal{M}\mathbf{e} \equiv \mathbf{0} \pmod 2$ other than $\mathbf{0}$.
- In other words we want the exponents in the prime factorisation of
$$f(x_1)^{e_1} \dots f(x_K)^{e_K}$$
to be even in a non-trivial way.

- The standard way of doing this is through Gaussian elimination, and it suffices to perform it modulo 2, although for the matrices which occur for large n, which are sparse there are faster methods. For the numbers used here Gauss' method will suffice.

- The standard way of doing this is through Gaussian elimination, and it suffices to perform it modulo 2, although for the matrices which occur for large n, which are sparse there are faster methods. For the numbers used here Gauss' method will suffice.
- On Class467-08T2.pdf I have listed the successive row operations, beginning with using the first row to eliminate the first entries in the other rows, and then using successive rows to eliminate the entries in the column corresponding to their leading entry.

- The standard way of doing this is through Gaussian elimination, and it suffices to perform it modulo 2, although for the matrices which occur for large n, which are sparse there are faster methods. For the numbers used here Gauss' method will suffice.
- On Class467-08T2.pdf I have listed the successive row operations, beginning with using the first row to eliminate the first entries in the other rows, and then using successive rows to eliminate the entries in the column corresponding to their leading entry.
- Here is the final form of the matrix, from which we can read off the equations for $\mathbf{e}$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$e_1 + e_8 \equiv 0 \pmod 2, \quad e_2 + e_{10} \equiv 0 \pmod 2,$$
$$e_3 + e_7 \equiv 0 \pmod 2, \quad e_4 + e_7 \equiv 0 \pmod 2,$$
$$e_5 + e_8 \equiv 0 \pmod 2, \quad e_6 + e_{10} \equiv 0 \pmod 2,$$
$$e_9 \equiv 0 \pmod 2.$$

- $$\begin{aligned} e_1 + e_8 &\equiv 0 \pmod 2, & e_2 + e_{10} &\equiv 0 \pmod 2,\\ e_3 + e_7 &\equiv 0 \pmod 2, & e_4 + e_7 &\equiv 0 \pmod 2,\\ e_5 + e_8 &\equiv 0 \pmod 2, & e_6 + e_{10} &\equiv 0 \pmod 2,\\ & & e_9 &\equiv 0 \pmod 2. \end{aligned}$$

- $$\begin{aligned} e_1 + e_8 &\equiv 0 \pmod 2, & e_2 + e_{10} &\equiv 0 \pmod 2,\\ e_3 + e_7 &\equiv 0 \pmod 2, & e_4 + e_7 &\equiv 0 \pmod 2,\\ e_5 + e_8 &\equiv 0 \pmod 2, & e_6 + e_{10} &\equiv 0 \pmod 2,\\ & & e_9 &\equiv 0 \pmod 2. \end{aligned}$$

- Thus taking e_7, e_8 and e_{10} as the independent variables we see that

$$\big(f(x_3)f(x_4)f(x_7)\big)^{e_7}\big(f(x_1)f(x_5)f(x_8)\big)^{e_8}\times \big(f(x_2)f(x_6)f(x_{10})\big)^{e_{10}}$$

is always a perfect square.

- $$\begin{aligned} e_1 + e_8 &\equiv 0 \pmod 2), & e_2 + e_{10} &\equiv 0 \pmod 2),\\ e_3 + e_7 &\equiv 0 \pmod 2), & e_4 + e_7 &\equiv 0 \pmod 2),\\ e_5 + e_8 &\equiv 0 \pmod 2), & e_6 + e_{10} &\equiv 0 \pmod 2),\\ & & e_9 &\equiv 0 \pmod 2). \end{aligned}$$

- Thus taking e_7, e_8 and e_{10} as the independent variables we see that
$$\big(f(x_3)f(x_4)f(x_7)\big)^{e_7}\big(f(x_1)f(x_5)f(x_8)\big)^{e_8}\times \big(f(x_2)f(x_6)f(x_{10})\big)^{e_{10}}$$
is always a perfect square.
- The choices $e_7 = 1, e_8 = e_{10} = 0$ and $e_8 = 1, e_7 = e_{10} = 0$ correspond to the solutions used above.

- $$\begin{aligned} e_1+e_8 &\equiv 0 \pmod 2, & e_2+e_{10} &\equiv 0 \pmod 2,\\ e_3+e_7 &\equiv 0 \pmod 2, & e_4+e_7 &\equiv 0 \pmod 2,\\ e_5+e_8 &\equiv 0 \pmod 2, & e_6+e_{10} &\equiv 0 \pmod 2,\\ && e_9 &\equiv 0 \pmod 2. \end{aligned}$$

- Thus taking e_7, e_8 and e_{10} as the independent variables we see that
$$\big(f(x_3)f(x_4)f(x_7)\big)^{e_7}\big(f(x_1)f(x_5)f(x_8)\big)^{e_8}\times \big(f(x_2)f(x_6)f(x_{10})\big)^{e_{10}}$$
is always a perfect square.
- The choices $e_7=1, e_8=e_{10}=0$ and $e_8=1, e_7=e_{10}=0$ correspond to the solutions used above.
- The solution $e_{10}=1, e_7=e_8=0$ does not give a factorization.

- Here is another example with a somewhat larger n.

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$*.*

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$.
- *We first need to check which primes* $p \leq 50$ *will occur in the method.*

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$*.*
- *We first need to check which primes* $p \leq 50$ *will occur in the method.*
- *Thus for each odd prime* $p \leq 50$ *we need to ascertain whether* n *is a QR or a QNR modulo* p*.*

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$.
- *We first need to check which primes* $p \le 50$ *will occur in the method.*
- *Thus for each odd prime* $p \le 50$ *we need to ascertain whether* n *is a QR or a QNR modulo* p.
- *By* **(LJ)** *we obtain a factor base*

$$\mathcal{P} = \{-1, 2, 3, 5, 11, 31, 47\}.$$

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$.
- *We first need to check which primes* $p \leq 50$ *will occur in the method.*
- *Thus for each odd prime* $p \leq 50$ *we need to ascertain whether* n *is a QR or a QNR modulo* p.
- *By* **(LJ)** *we obtain a factor base*

$$\mathcal{P} = \{-1, 2, 3, 5, 11, 31, 47\}.$$

- *We have* $\sqrt{n} \approx 2340$. *For larger numbers such as* n *it is harder to obtain complete factorisations of* $f(x) = x^2 - n$.

- Here is another example with a somewhat larger n.
- **Example 8.3.** *Let* $n = 5479879$ *and take the sieving limit* $B = 50$.
- *We first need to check which primes* $p \leq 50$ *will occur in the method.*
- *Thus for each odd prime* $p \leq 50$ *we need to ascertain whether* n *is a QR or a QNR modulo* p.
- *By* **(LJ)** *we obtain a factor base*

$$\mathcal{P} = \{-1, 2, 3, 5, 11, 31, 47\}.$$

- *We have* $\sqrt{n} \approx 2340$. *For larger numbers such as* n *it is harder to obtain complete factorisations of* $f(x) = x^2 - n$.
- *Either the range for* x *has to be increased, or alternatively extend the factor base* $\mathcal{P}$.

- See Class467-08T3.pdf.

- See Class467-08T3.pdf.
- Now we extract the parity of the exponents for each prime and form the matrix

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- See Class467-08T3.pdf.
- Now we extract the parity of the exponents for each prime and form the matrix

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- We now apply Gaussian elimination and obtain

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- $$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- $$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$
- Thus we find that
$$\begin{aligned} e_1 + e_4 &\equiv 0 \pmod 2, \\ e_2 + e_4 + e_5 &\equiv 0 \pmod 2, \\ e_3 + e_5 &\equiv 0 \pmod 2, \\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

- Thus we find that

$$\begin{aligned} e_1 + e_4 &\equiv 0 \pmod 2, \\ e_2 + e_4 + e_5 &\equiv 0 \pmod 2, \\ e_3 + e_5 &\equiv 0 \pmod 2, \\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

- Thus we find that

$$\begin{aligned} e_1 + e_4 &\equiv 0 \pmod 2, \\ e_2 + e_4 + e_5 &\equiv 0 \pmod 2, \\ e_3 + e_5 &\equiv 0 \pmod 2, \\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

- We can take e_4, e_5 and e_6 as the independent variables.

- Thus we find that

$$\begin{aligned} e_1 + e_4 &\equiv 0 \pmod 2,\\ e_2 + e_4 + e_5 &\equiv 0 \pmod 2,\\ e_3 + e_5 &\equiv 0 \pmod 2,\\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

- We can take e_4, e_5 and e_6 as the independent variables.
- Taking e_4 and e_5 as the independent variables we see that

$$\begin{aligned} e_1 &\equiv e_4 \pmod 2,\\ e_2 &\equiv e_4 + e_5 \pmod 2,\\ e_3 &\equiv e_5 \pmod 2,\\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

- Taking e_4 and e_5 as the independent variables we see that

$$e_1 \equiv e_4 \pmod 2,$$
$$e_2 \equiv e_4 + e_5 \pmod 2,$$
$$e_3 \equiv e_5 \pmod 2,$$
$$e_6 \equiv 0 \pmod 2,$$

- Taking e_4 and e_5 as the independent variables we see that

$$e_1 \equiv e_4 \pmod 2,$$
$$e_2 \equiv e_4 + e_5 \pmod 2,$$
$$e_3 \equiv e_5 \pmod 2,$$
$$e_6 \equiv 0 \pmod 2,$$

- and so each of

$$f(x_1)f(x_2)f(x_4),$$
$$f(x_2)f(x_3)f(x_5),$$

is a perfect square.

- Each of the following are squares.

$$f(x_1)f(x_2)f(x_4),$$
$$f(x_2)f(x_3)f(x_5),$$

- Each of the following are squares.

$$f(x_1)f(x_2)f(x_4),$$
$$f(x_2)f(x_3)f(x_5),$$

- We have

$$x_1 \times x_2 \times x_4 = 2198 \times 2225 \times 2373 = 11605275150$$

$$\begin{aligned} f(x_1)f(x_2)f(x_4) &= (-1)^2 \times 2^2 \times 3^{10} \times 5^6 \times 11^4 \times 31^2 \\ &= (2 \times 3^5 \times 5^3 \times 11^2 \times 31)^2 = 227873250^2 \end{aligned}$$

- Each of the following are squares.

$$f(x_1)f(x_2)f(x_4),$$
$$f(x_2)f(x_3)f(x_5),$$

- We have

$$x_1 \times x_2 \times x_4 = 2198 \times 2225 \times 2373 = 11605275150$$

$$\begin{aligned} f(x_1)f(x_2)f(x_4) &= (-1)^2 \times 2^2 \times 3^{10} \times 5^6 \times 11^4 \times 31^2 \\ &= (2 \times 3^5 \times 5^3 \times 11^2 \times 31)^2 = 227873250^2 \end{aligned}$$

- Thus

$$\begin{aligned} &(11605275150 - 227873250, n) \\ &\qquad = (11377401900, 5479879) = 5431 \end{aligned}$$

and

$$(1105275150 + 227873250, 5479879) = 1009.$$

- We can also check the second relationship.

$$x_2 \times x_3 \times x_5 = 2225 \times 2252 \times 2383 = 11940498100$$

$$\begin{aligned} f(x_2)f(x_3)f(x_5) &= (-1)^2 \times 2^2 \times 3^{12} \times 5^4 \times 11^4 \times 47^2 \\ &= (2 \times 3^6 \times 5^2 \times 11^2 \times 47)^2 = 207291150^2 \end{aligned}$$

Then

$$\begin{aligned} 11940498100 - 207291150 &= 11733206950, \\ 11940498100 + 207291150 &= 12147789250, \end{aligned}$$

$$(11733206950, 5479879) = 1009$$

and

$$(12147789250, 5479879) = 5431.$$

Note on Gaussian Elimination

- As part of the quadratic sieve we need to solve systems of linear congruences of the kind

$$\begin{aligned} a_{11}e_1 + a_{12}e_2 + \cdots + a_{1m}e_m &\equiv 0 \pmod 2, \\ a_{21}e_1 + a_{22}e_2 + \cdots + a_{2m}e_m &\equiv 0 \pmod 2, \\ \vdots \qquad\qquad & \qquad \vdots \\ a_{l1}e_1 + a_{l2}e_2 + \cdots + a_{lm}e_m &\equiv 0 \pmod 2. \end{aligned}$$

Note on Gaussian Elimination

- As part of the quadratic sieve we need to solve systems of linear congruences of the kind

$$\begin{aligned} a_{11}e_1 + a_{12}e_2 + \cdots + a_{1m}e_m &\equiv 0 \pmod 2, \\ a_{21}e_1 + a_{22}e_2 + \cdots + a_{2m}e_m &\equiv 0 \pmod 2, \\ &\vdots \\ a_{l1}e_1 + a_{l2}e_2 + \cdots + a_{lm}e_m &\equiv 0 \pmod 2. \end{aligned}$$

- In our situation the a_{jk} can be taken to be 1 or 0 which simplifies computation.

Note on Gaussian Elimination

- As part of the quadratic sieve we need to solve systems of linear congruences of the kind

$$\begin{aligned}
a_{11}e_1 + a_{12}e_2 + \cdots + a_{1m}e_m &\equiv 0 \pmod 2,\\
a_{21}e_1 + a_{22}e_2 + \cdots + a_{2m}e_m &\equiv 0 \pmod 2,\\
&\vdots \qquad\qquad \vdots\\
a_{l1}e_1 + a_{l2}e_2 + \cdots + a_{lm}e_m &\equiv 0 \pmod 2.
\end{aligned}$$

- In our situation the a_{jk} can be taken to be 1 or 0 which simplifies computation.
- For the numbers we will deal with Gaussian elimination is adequate, and has the merit of being straightforward.

Note on Gaussian Elimination

$$\begin{aligned}
a_{11}e_1 + a_{12}e_2 + \cdots + a_{1m}e_m &\equiv 0 \pmod 2,\\
a_{21}e_1 + a_{22}e_2 + \cdots + a_{2m}e_m &\equiv 0 \pmod 2,\\
&\vdots \qquad\qquad \vdots\\
a_{l1}e_1 + a_{l2}e_2 + \cdots + a_{lm}e_m &\equiv 0 \pmod 2.
\end{aligned}$$

- We can write this more succinctly in matrix notation as

$$\mathcal{A}\mathbf{e} = \mathbf{0}$$

where

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m}\\ a_{21} & a_{22} & \cdots & a_{2m}\\ \vdots & \vdots & & \vdots\\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}, \quad \mathbf{e} = \begin{pmatrix} e_1\\ e_2\\ \vdots\\ e_m \end{pmatrix}, \quad \mathbf{0} = \begin{pmatrix} 0\\ 0\\ \vdots\\ 0 \end{pmatrix}$$

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

- The first observation that can be made is that it is immaterial as to the order in which we write the equations so at any state we can interchange them if it is convenient to do so. Thus we can suppose initially that a left-most non-zero entry is in the top row. This is sometimes called a *pivot*.

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

- The first observation that can be made is that it is immaterial as to the order in which we write the equations so at any state we can interchange them if it is convenient to do so. Thus we can suppose initially that a left-most non-zero entry is in the top row. This is sometimes called a *pivot*.
- Our second observation is that in our original system of linear congruences we can take one equation and subtract it from another. This is equivalent to taking the corresponding row in the matrix and subtracting it from the second corresponding row.

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

- When Gaussian elimination is applied generally in the real world one can even take real multiples of one row from another, but in this world we have the much simple environment of having only zeros and ones. Note that if subtraction gives -1 this is the same as 1.

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

- When Gaussian elimination is applied generally in the real world one can even take real multiples of one row from another, but in this world we have the much simple environment of having only zeros and ones. Note that if subtraction gives -1 this is the same as 1.
- Denote the pivot in the top row by a_{j1}. We now take the first row and subtract it from every row with $a_{jk} = 1$. Thus the new matrix will have $a_{j1} = 1$ and all the entries to the left and below it are 0.

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

- When Gaussian elimination is applied generally in the real world one can even take real multiples of one row from another, but in this world we have the much simple environment of having only zeros and ones. Note that if subtraction gives -1 this is the same as 1.
- Denote the pivot in the top row by a_{j1}. We now take the first row and subtract it from every row with $a_{jk} = 1$. Thus the new matrix will have $a_{j1} = 1$ and all the entries to the left and below it are 0.
- We now repeat this process with the submatrix formed from the rows $j + 1$ through m.

- We continue in this way until we have reduced the matrix to *echelon* form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- We continue in this way until we have reduced the matrix to *echelon* form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- Note that the matrix might well have zeros on the diagonal from some point on. If so some of the rows at the bottom of the matrix are likely to consist of all zeros.

- We continue in this way until we have reduced the matrix to *echelon* form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- Note that the matrix might well have zeros on the diagonal from some point on. If so some of the rows at the bottom of the matrix are likely to consist of all zeros.
- The first 1 in a row is called a *pivot*.

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- Starting from the bottom of the matrix we now use these pivots to remove any non-zero entry above the pivot.

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- Starting from the bottom of the matrix we now use these pivots to remove any non-zero entry above the pivot.
- Thus the last matrix would take on the shape

$$\begin{pmatrix} 1 & 0 & a_{13} & 0 & \cdots & a_{1m} \\ 0 & 1 & a_{23} & 0 & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- Starting from the bottom of the matrix we now use these pivots to remove any non-zero entry above the pivot.
- Thus the last matrix would take on the shape

$$\begin{pmatrix} 1 & 0 & a_{13} & 0 & \cdots & a_{1m} \\ 0 & 1 & a_{23} & 0 & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- This is called *reduced echelon* form.

$$\begin{pmatrix} 1 & 0 & a_{13} & 0 & \cdots & a_{1m} \\ 0 & 1 & a_{23} & 0 & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

- The variables corresponding to pivots are the dependent variables and the other variables are the independent ones. The values for the dependent variables are then easily read off in terms of the independent ones.

- Thus in Example 8.1 the reduced echelon form is

$$\begin{pmatrix}1&0&0&0&0&0&0&1&0&0\\0&1&0&0&0&0&0&0&0&1\\0&0&1&0&0&0&1&0&0&0\\0&0&0&1&0&0&1&0&0&0\\0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0\end{pmatrix}$$

e_1, e_2, e_3, e_4, e_5, e_6 and e_9 are dependent variables and the e_7, e_8 and e_{10} can be chosen at random.