- It is known that the corresponding convergents $\{a_0, x_1/y_1, x_2/y_2, \dots\}$ give improving approx. to $\sqrt{n}$ & satisfy:

$$Q_i := x_i^2 - n y_i^2 \,, \quad |Q_i| < 2\sqrt{n}.$$

- Since Q_i's are "small", one hopes to quickly find $i_1 < i_2 < \dots < i_k$ s.t. $Q_{i_1} \cdots Q_{i_k}$ is a square v^2.

$$\Rightarrow \quad Q_{i_1} \cdots Q_{i_k} \equiv (x_{i_1} \cdots x_{i_k})^2 \equiv v^2 \pmod{n}.$$

Morrison & Brillhart's implementation (1970)

- Idea is to use Q_i's, from the continued fraction of $\sqrt{n}$, that are B-smooth.

Input: non-square $n \in \mathbb{N}_{>2}$.

Output: Factoring n.

1) Fix a bound B. Let $\{p_1, \dots, p_B\}$ be the first B prime numbers. * factor-base

2) Compute the set $S := \{Q_i \mid Q_i = (-1)^{\alpha_{i0}} p_1^{\alpha_{i1}} \cdots p_B^{\alpha_{iB}}$, for some $\alpha_{ij} \geq 0\}$ s.t. $|S| = B+2$.

($Q_i = x_i^2 - n \cdot y_i^2$)

3) Consider the $B+2$ vectors $\{(\alpha_{i0}, \ldots, \alpha_{iB}) \mid Q_i \in S\}$. ($= \overline{\alpha_i}$)

Compute a subset $T \subseteq S$ s.t. the vectors $\{\overline{\alpha_i} \mid Q_i \in T\}$ sum to $0 \pmod 2$.

4) So, we have: $\prod_{Q_i \in T} Q_i$ is a square v^2.

5) OUTPUT $\gcd\left(\prod_{Q_i \in T} x_i - v, n\right)$.

Assumption: $\{Q_i = x_i^2 - n \cdot y_i^2 \mid i > 0\}$ is a random sequence.

Theorem: Heuristically, the algorithm takes time
$\exp\left((o(1)+\sqrt{2}) \cdot \sqrt{\lg n \cdot \lg\lg n}\right) = L_n\left(\frac{1}{2}, \sqrt{2}+o(1)\right)$.

Proof:

- $\Pr[Q_i$ is p_B-smooth$] \approx \Psi(\sqrt{n}, p_B)/\sqrt{n}$
- $\Rightarrow$ The expected # i's after which we

will get $(B+2)$ smooth $Q_{\hat{i}}$'s

$$\approx B \cdot \sqrt{n} / \psi(\sqrt{n}, p_B)$$

- Total time is dominated by the p_B-smoothness check, which requires $\approx B^2 \cdot \sqrt{n}/\psi(\sqrt{n}, p_B)$ time.

- Setting $B = L_{\sqrt{n}}(\alpha, c)$ this becomes

$$\approx L_{\sqrt{n}}(\alpha, c)^2 \cdot L_{\sqrt{n}}\left(1-\alpha, \frac{1-\alpha}{c}\right)$$

$$= e^{2 \cdot c \cdot (\log \sqrt{n})^{\alpha} \cdot (\log\log \sqrt{n})^{1-\alpha} + \frac{1-\alpha}{c} \cdot (\log \sqrt{n})^{1-\alpha} \cdot (\log\log \sqrt{n})^{\alpha}}$$

- which is minimized, at $\alpha = c = 1/2$, to:

$$\approx \exp\left(\sqrt{2 \cdot \log n \cdot \log\log n}\right) = L_n\left(\tfrac{1}{2}, \sqrt{2}\right).$$

- $B \approx \exp\left(\frac{1}{2\sqrt{2}} \cdot \sqrt{\log n \cdot \log\log n}\right) = L_n\left(\tfrac{1}{2}, \frac{1}{2\sqrt{2}}\right)$. □

Success: $F_7 = 2^{128}+1$ was factored into two primes (17 & 22 digits), amongst other ≤70 digit numbers.

C.frac. of $\sqrt{257 F_7}$ was used.

Quadratic Sieve

- Pomerance (1981) suggested a <u>sieving</u> idea to reduce the time taken to test <u>smoothness</u>.

Also, the C.frac. method is too "sequential". It was replaced by $Q(x) = x^2 - n$ where x is kept close to $\sqrt{n}$.

<u>Modifications</u>:

1) In the above algorithm compute the list of $Q(x) = x^2 - n$ for $N := B \cdot \sqrt{n} / \psi(\sqrt{n}, p_B)$ x's above $\lfloor \sqrt{n} \rfloor$.

2) Check their <u>smoothness</u> as:

For $1 \leq i \leq B$:

Look at $2N/p_i$ places in the list that are divisible by p_i. <u>Modify</u> the list by dividing these by the highest power of p_i.

3) The places in the list, with value $= 1$,

indicate the i's where $\{Q(\lfloor\sqrt{n}\rfloor+i)\}$ is p_B-smooth.

- Time taken now $\approx \sum_{i=1}^{B} \frac{2N}{p_i} \approx N \cdot \log\log B$
$\approx B \cdot \log\log B \cdot \sqrt{n}/\psi(\sqrt{n}, p_B)$
$\approx L_{\sqrt{n}}(\alpha, c) \cdot L_{\sqrt{n}}(1-\alpha, \frac{1-\alpha}{c})$, for $B = L_{\sqrt{n}}(\alpha, c)$.

- This gets minimized, at $(\alpha, c) = (\frac{1}{2}, \frac{1}{\sqrt{2}})$, to:
$\approx L_{\sqrt{n}}(\frac{1}{2}, \frac{1}{\sqrt{2}}) \cdot L_{\sqrt{n}}(\frac{1}{2}, \frac{1}{\sqrt{2}})$
$\approx L_n(\frac{1}{2}, 1)$,
for $B \approx L_n(\frac{1}{2}, \frac{1}{2})$.

- The drop of $\sqrt{2}$ from the exponent leads to a <u>two-fold</u> increase in the length of n that can be factored!

<u>Success:</u> Lenstra & Manasse (1994) factored a 129-digit RSA challenge using distributed computing over the Internet.

Number field sieve (NFS)

- Pollard (1988) suggested using algebraic number fields to factor numbers of the form x^3+k, for small k & large x.

  Lenstra, Lenstra & Manasse (1990) improved it & factored $F_9 = 2^{512}+1$ into 3 primes (7, 49, 99 digits).

Idea: • Quadratic sieve devises equalities of the form $\prod_{i=1}^{k}(x_i^2 - n y_i^2) = v^2$ over $\mathbb{Z}$.

• Using the norm $\mathcal{N}: \mathbb{Q}(\sqrt{n}) \to \mathbb{Q}$ we can rewrite it as: $\prod_i \mathcal{N}(x_i - y_i\sqrt{n}) = \mathcal{N}\left(\prod_i (x_i - y_i\sqrt{n})\right) = v^2$.

• Its high-order generalization is to go to a number field $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/\langle f \rangle$, where f is an irreducible polynomial of degree $(d+1)$.