

# SQUFOF.

We wish to factor the odd positive integer  $D$ . We assume proved that  $D$  is composite, via a Miller-test to several bases.

Let  $p_k/q_k$  be the  $k$ :th convergent in the continued fractions expansion of  $\sqrt{D}$ ,  $D$  odd, and let  $Q_k$  be the denominator of  $\alpha_k$  as found by Bhaskara. If  $k + 1$  is even, then

$$p_k^2 - Dq_k^2 = Q_{k+1}.$$

We know that  $Q_{k+1} < 2\sqrt{D}$ , while  $p_k, q_k$  can be very large, even on reduction modulo  $D$ .

With luck  $Q_{k+1} = R^2$ , so that  $D|(p_k^2 - R^2) = (p_k - R)(p_k + R)$  and with even more luck  $D \nmid p_k - R$  or  $D \nmid p_k + R$ . Then  $(D, p_k - R)$  or  $(D, p_k + R)$  will be a proper factor of  $D$ .

It can be proved that this will hold exactly if (after an even number of steps)  $Q_{k+1} = R^2$ , where  $R$  (odd) or  $2R$  has not appeared as an earlier  $Q_j$ .

One strategy therefore is to store  $Q_k$  (odd) or  $Q_k/2$  ( $Q_k$  even) in a list. If the expansion then produces an  $Q_l$ ,  $l$  even, such that  $Q_l$  is a perfect square,  $\sqrt{Q_l}$  not in the list (the “queue”) one obtains a non-trivial factorization.

Note that only those  $Q_k$  for which  $Q_k < \sqrt{8}D^{1/4}$  need be included in the queue, as  $Q_l < 2\sqrt{D}$ .

Daniel Shanks (1917-1996) observed around 1975 that one need not compute the  $p_k, q_k$ . He showed this by using the somewhat hairy theory of binary quadratic forms, going all the way back to Gauß. He called his algorithm Square Forms Factorization, SQUFOF.

Riesel observed in his book that Shanks’ algorithm – somewhat modified – can be formulated in the language of continued fractions. He does not prove it, though, and in this form the algorithm runs a bit slower.

I have spent a couple of days devising the following proof. Simplifications are welcome!

## We Set Things in Motion

We assume  $k + 1$  even,  $Q_{k+1} = R^2$ , subject to the constraints given above. Then

$$\alpha_{k+1} = \frac{P + \sqrt{D}}{R^2},$$

where  $R^2 | (D - P^2)$ . By our equivalence theory

$$\sqrt{D} = \frac{p\alpha_{k+1} + q}{r\alpha_{k+1} + s} = \frac{p(P + \sqrt{D}) + qR^2}{r(P + \sqrt{D}) + sR^2},$$

whence

$$\alpha_{k+1} = \frac{s\sqrt{D} - q}{-r\sqrt{D} + p}, \quad ps - qr = +1.$$

(The plus sign comes from  $k + 1$  being even.) As in the derivation of Pell's equation we are led to the the following identifications:

$$\begin{aligned} p &= rP + sR^2 \\ Dr &= pP + qR^2 \end{aligned}$$

whence  $p^2 - Dr^2 = R^2$ . From the general theory follows that  $p/r$  is the last convergent of the expansion (and  $q/s$  the next to last one).

## Another Equivalence

We now set

$$\beta_0 = \frac{R}{\sqrt{D} - P}, \quad \gamma_0 = \frac{-1}{\beta'_0} = \frac{P + \sqrt{D}}{R}.$$

It could occur that these entities are not reduced.

However, if we start an expansion from  $\beta_0$ , then  $\beta_1$  and  $\gamma_1 = -1/\beta'_1$  are reduced, as  $\beta'_0$  is negative. The one exception is the case  $0 < \beta_0 < 1$ , but then  $\beta_1 > 1$ ,  $\beta'_1 < 0$  anyway, and  $\beta_2$  is reduced.

We now prove that  $\beta_0, \gamma_0$  are equivalent via a matrix of determinant  $= -1$ . Then the same holds for the reduced quantities  $\beta_1, \gamma_1$ , as they are produced

in one single step (determinant =  $-1$ ) from  $\beta_0, \gamma_0$  (or, in the exceptional case,  $\beta_2, \gamma_2 = -1/\beta_2'$ , produced in two steps, determinant =  $1$ ).

By the proof of the equivalence criterion this means that  $\gamma_1$  is reached from  $\beta_1$  (alt.  $\gamma_2$  is reached from  $\beta_2$ ) *by a continued fractions expansion*, in an odd number of steps, a fact that will lead to factoring  $D$ .

We connect with the previous equivalence, setting

$$\begin{pmatrix} t & u \\ v & w \end{pmatrix} = \frac{1}{R} \begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -P \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & R \end{pmatrix}$$

A simple determinant calculation shows that

$$tw - uv = \frac{1}{R^2} \cdot R \cdot (-1) \cdot 1 \cdot R = -1$$

The matrix above has integer elements. Using  $p - Pr = sR^2$ , a short computation shows that

$$\begin{pmatrix} t & u \\ v & w \end{pmatrix} = \begin{pmatrix} r & sR \\ sR & q - sP \end{pmatrix}$$

We now show that this matrix affords the transition

$$\text{from } \beta_0 = \frac{R}{\sqrt{D} - P} \text{ to } \frac{\sqrt{D} + P}{R} = \gamma_0$$

by interpreting the steps.

First of all

$$\begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -P \end{pmatrix} = \begin{pmatrix} 0 & R \\ 1 & -P \end{pmatrix} : \quad \frac{R}{\sqrt{D} - P} = \frac{0 \cdot \sqrt{D} + 1 \cdot R}{1 \cdot \sqrt{D} - P \cdot 1}$$

corresponding to the transition  $\beta_0 \rightarrow \sqrt{D}$ .

The middle factor

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

was the one taking us from  $\sqrt{D}$  to  $(\sqrt{D} + P)/R^2$ .

And

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

4

is the division by  $R$ :

$$\frac{\sqrt{D} + P}{R^2} = \frac{1}{R} \frac{\sqrt{D} + P}{R}$$

The scalar factor  $1/R$ , to the far left in the matrix product, cancels on division of the two components.

## Putting Everything Together

We now know there is a continued fractions expansion, in an odd number of steps:

$$\beta_1 \rightarrow \beta_2 \rightarrow \dots \gamma_2 = \beta_{2k-1} \rightarrow \gamma_1 = \beta_{2k}$$

where the first and last quantities are to be omitted in the exceptional case. We leave it to the reader to modify the following discussion to that case.

Now

$$\beta_{2k} = \gamma_1 = \frac{-1}{\beta'_1}$$

whence (by the symmetry properties established in the general theory)

$$\beta_{2k-1} = \frac{-1}{\beta'_2}, \dots, \beta_{k+1} = \frac{-1}{\beta'_k}$$

So the situation is:

$$\beta_k = \frac{P'_k + \sqrt{D}}{Q'_k} \rightarrow \beta_{k+1} = \frac{Q'_k}{-P'_k + \sqrt{D}} = \frac{P'_k + \sqrt{D}}{Q'_{k+1}},$$

so that

$$P'_{k+1} = P'_k.$$

By Bhaskara,  $Q'_k Q'_{k+1} = D - (P'_{k+1})^2$  and  $Q'_k | (P'_{k+1} + P'_k) = 2P'_k$ .

( $Q'_k | P'_k$  if  $Q'_k$  is odd.)

In the next paragraph we will show that  $Q'_k \neq 1$  and  $\neq 2$ .

But from  $Q'_k | (D - P'^2_k)$  and  $Q'_k | P'_k$  or  $Q'_k | 2P'_k$  then follows that  $Q'_k$  or  $Q'_k/2$  is a proper factor in  $D$  !!!

## Exclusion of Trivial Cases

The impatient reader will skip this somewhat tedious discussion and skip to the Example below.

Let us examine the structure. We have the following matrix factorization

$$\begin{aligned} \begin{pmatrix} t & u \\ v & w \end{pmatrix} &= \begin{pmatrix} r & sR \\ sR & q - sP \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \\ &= \begin{pmatrix} ma^2 + 2ac & mab + ad + bc \\ mab + ad + bc & mb^2 + 2bd \end{pmatrix} \end{aligned}$$

The first matrix represents the step from  $\beta_0$  to  $\beta_k$ , the second one represents  $\beta_k \rightarrow \beta_{k+1}$  and the last one represents  $\beta_{k+1} \rightarrow \gamma_0$ .

The first and third factors being transposes of one another reflects the symmetry revealed by the general theory.

Note that  $a, b, c, d > 0$ . Also note that  $ad + bc = ad - bc + 2bc = \pm 1 + 2bc$  is odd. Finally note that two matrix elements in the same row or column are relatively prime as the determinant equals  $\pm 1$ .

**Case I:**  $Q'_k = 1, \beta_k = \sqrt{D} + n$

As  $\beta_k$  is reduced,  $n = \lfloor \sqrt{D} \rfloor$ . Therefore  $\lfloor \beta_k \rfloor = 2n$ , and

$$\beta_{k+1} = \frac{1}{\beta_k - 2n}, \quad \beta_k = 2n + \frac{1}{\beta_{k+1}} = \frac{2n\beta_{k+1} + 1}{\beta_{k+1}}$$

so  $m = 2n$  is even,  $mab + ad + bc$  odd, and then it follows that  $R$  is *odd*, being a factor in  $mab + ad + bc$ .

The transition from  $\sqrt{D}$  to  $\beta_{k+1}$  is afforded by the matrix

$$\begin{pmatrix} n & 1 \\ 1 & 0 \end{pmatrix}, \text{ as } \sqrt{D} = n + \frac{1}{\beta_{k+1}}$$

so the transition from  $\sqrt{D}$  to  $\gamma_0$  is given by the product

$$\begin{pmatrix} n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} na + c & nb + d \\ a & b \end{pmatrix},$$

i.e.,

$$\sqrt{D} = \frac{(na + c)(\sqrt{D} + P) + (na + b)R}{a(\sqrt{D} + P) + bR}$$

The usual identifications lead to

$$(na + c)^2 - a^2D = \pm R$$

Here  $R < 2 \cdot D^{1/4} < \sqrt{D}$ . The numbers  $na + c$ ,  $a$  are relatively prime since  $a$ ,  $c$  are. Hence  $(na + c)/a$  is a convergent in the expansion of  $\sqrt{D}$ . We already know that  $p^2 - Dr^2 = R^2$ . From the matrix factorization above,  $r > a$ . Recall that  $R$  is odd.

But then  $R$  would have appeared before  $R^2$  in the expansion of  $\sqrt{D}$ . We have excluded that case. Therefore  $Q'_k \neq 1$ .

**Case II:**  $Q'_k = 2, \beta_k = (\sqrt{D} + n)/2$ ,  $n$  even

We easily verify that  $[\beta_k] = n$ , so this time, too,  $m$  is even, and  $R$  is odd.

The transition from  $\sqrt{D}$  to  $\gamma_0$  is now given by the matrix

$$\begin{pmatrix} n & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} na + 2c & nb + 2d \\ a & b \end{pmatrix}$$

The first factor follows from

$$\sqrt{D} = n + \frac{2}{\beta_{k+1}}$$

The same identification as many times before yields:

$$(na + 2c)^2 - Da^2 = \pm 2R$$

Here  $(na + 2c, a) = (2c, a) = 1$  or  $2$ . But in the latter case the left member would be divisible by 4, contradicting the fact that  $R$  is odd.

So we can exclude this case in the same way as the previous one.

**Case III:**  $Q'_k = 2, \beta_k = (\sqrt{D} + n)/2$ ,  $n$  odd.

It still holds that  $[\beta_k] = n$ , however,  $n$  is odd this time.

We still obtain the matrix

$$\begin{pmatrix} n & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} na + 2c & nb + 2d \\ a & b \end{pmatrix}$$

and

$$(na + 2c)^2 - Da^2 = \pm 2R$$

with  $(na + 2c, a) = (2c, a) = 1$  or  $2$ . But  $a$  even would imply  $b, c$  odd, and  $sR = mab + ad + bc$  odd, hence also  $R$  odd and we arrive at the same contradiction as in Case II.

And if  $a$  is odd, then  $(na + 2c, a) = 1$  and we arrive at the same conclusions as before.

## A Computer Run

We use Riesel's example  $D = 1000009$  (accessible, of course, by trial division), but give all the details absent from his account.

The floor of  $\sqrt{D}$  is 1000. Bhaskara gives:

$j$	$P_j$	$Q_j$	$a_j$
1	1000	9	222
2	998	445	4
3	782	873	2
4	964	81	24
5	980	489	4
6	976	97	20
7	964	729	2
8	494	1037	1
9	543	680	2
10	817	489	3
11	650	1181	1
12	531	608	2
13	685	873	1
14	188	1105	1
15	917	144	13
16	955	611	3
17	878	375	5
18	997	16	124

The denominator  $81 = 9^2$ , after 4 steps, cannot be used, as 9 has already appeared. But  $16 = 4^2$  works fine.

We thus have to perform the continued fractions expansion of

$$\beta_0 = \frac{4}{\sqrt{D} - 997} = \frac{\sqrt{D} + 997}{1500},$$

8

thus:

$j$	$P'_j$	$Q'_j$	$a'_j$
1	503	498	3
2	991	36	55
3	989	608	3
4	835	498	3
5	659	1136	1
6	477	680	2
7	883	324	5
8	737	1410	1
9	673	388	4
10	879	586	3
11	879	388	5

Here we get our repeat,  $P'_{10} = P'_{11}$ , and  $Q'_{10}/2 = 586/2 = 293$  is the desired factor.

We obtain the factorization

$$D = 1000009 = 293 \cdot 3413$$