Number Theory And Algebra

CONTINUED FRACTION FACTORIZATION ALGORITHM

GOKUL – CB.EN.U4CYS21018

SOURABH – CB.EN.U4CYS21071

NITIN – CB.EN.U4CYS21017

PRANAV – CB.EN.U4CYS21056

INIYAN – CB.EN.U4CYS21023

NISHANTH – CB.EN.U4CYS21050

SARANESH – CB.EN.U4CYS21068

MANOMITHRAN – CB.EN.U4CYS21040

VINAYAK – CB.EN.U4CYS21084

ACHYUTH – CB.EN.U4CYS21002

Why is Factoring Important?

The security of some of the most commonly used encryption schemes such as the RSA encryption scheme is proportional to the difficulty of factoring large integers quickly. Consequently, if you can create a ”fast” algorithm for factoring integers, then the RSA encryption scheme will no longer be secure. Alternatively, if you can determine a lower bound for the run time of any integer factoring algorithm, then you will have proven a lower bound on the security of the RSA encryption scheme.

Why is the Continued Fraction Factoring Method Important?

The continued fraction method is perhaps the first modern general purpose integer factorization method.

The Continued Fraction Factoring Method was used by John Brillhart and Michael Morrison on September 13, 1970, in order to discover that $2^{128} + 1 = 59649589127497217 \cdot 5704689200685129054721$

Continued Fraction of Rational Numbers

Let a and b be integers and let Euclid's algorithm run as:

$a = bq_0 + r_1$

$b = r_1q_1 + r_2,$

$c = r_2q_2 + r_3,$

. . . .

. . . .

$r_{n-1} = r_nq_n + 0$

Then the fraction a/b can be expressed as:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots\, q_{n-1} + \cfrac{1}{q_n}}}}$$

Continued Fractions of Rational Numbers

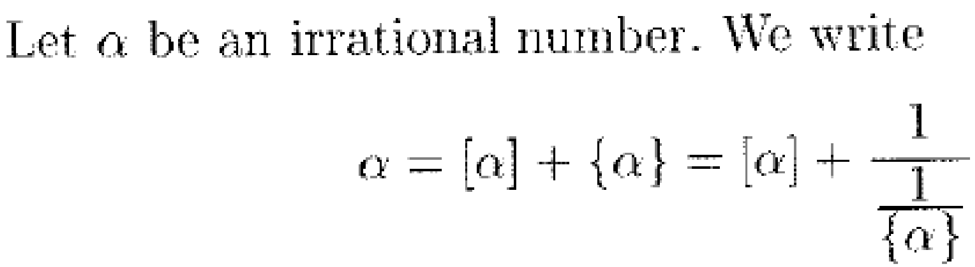
245/96

$$245 = 2 \cdot 96 + 53$$
$$96 = 1 \cdot 53 + 43$$
$$53 = 1 \cdot 43 + 10$$
$$43 = 4 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

$$\frac{245}{96} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{3}}}}}$$

Continued Fractions of Irrational Numbers

Let q_0, q_1, q_2, …. be a sequence of integers, all positive. Then the expression $[q_0, q_1, q_2, \ldots]$ is called an infinite simple continued fraction.

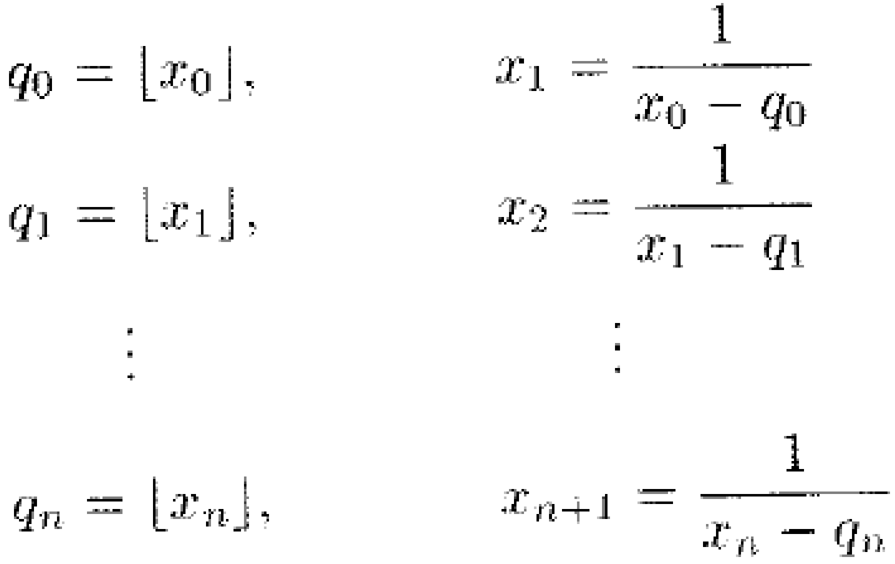


Let α be an irrational number. We write

$$\alpha = [\alpha] + \{\alpha\} = [\alpha] + \frac{1}{\frac{1}{\{\alpha\}}}$$

Where [a] is the integral part and {a} is the fractional part.

Let x = x_0 be a real number. Then α can be expressed as a simple continued fraction by the following process:



$$q_0 = \lfloor x_0 \rfloor, \qquad x_1 = \frac{1}{x_0 - q_0}$$

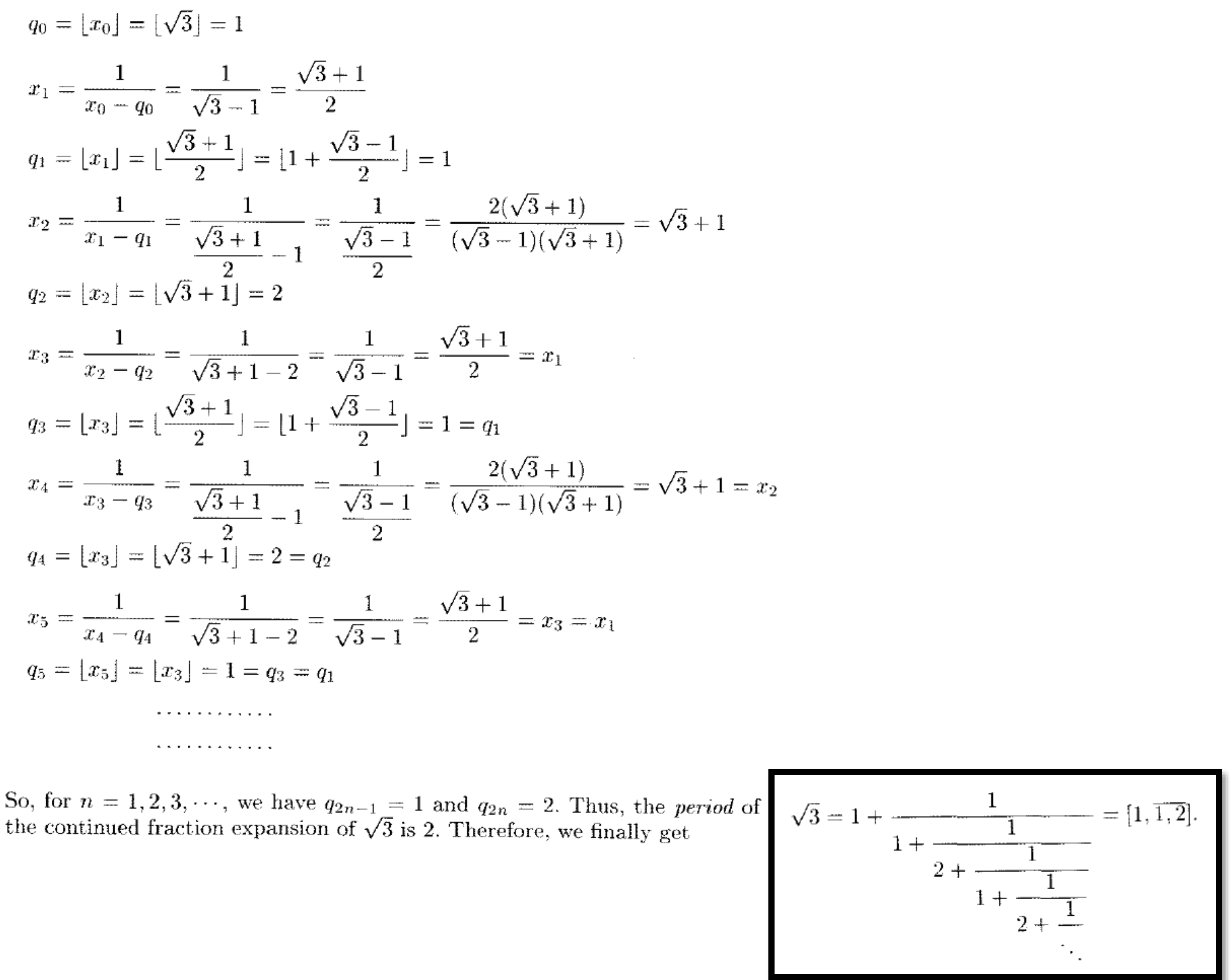
$$q_1 = \lfloor x_1 \rfloor, \qquad x_2 = \frac{1}{x_1 - q_1}$$

$$\vdots \qquad\qquad \vdots$$

$$q_n = \lfloor x_n \rfloor, \qquad x_{n+1} = \frac{1}{x_n - q_n}$$

Continuous Fractions of Irrational Numbers

Expand 3 as a periodic simple continued fraction. Let $x_0 = \sqrt{3}$. Then we have:



$$q_0 = \lfloor x_0 \rfloor = \lfloor \sqrt{3} \rfloor = 1$$

$$x_1 = \frac{1}{x_0 - q_0} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

$$q_1 = \lfloor x_1 \rfloor = \lfloor \frac{\sqrt{3}+1}{2} \rfloor = \lfloor 1 + \frac{\sqrt{3}-1}{2} \rfloor = 1$$

$$x_2 = \frac{1}{x_1 - q_1} = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \frac{1}{\frac{\sqrt{3}-1}{2}} = \frac{2(\sqrt{3}+1)}{(\sqrt{3}-1)(\sqrt{3}+1)} = \sqrt{3}+1$$

$$q_2 = \lfloor x_2 \rfloor = \lfloor \sqrt{3}+1 \rfloor = 2$$

$$x_3 = \frac{1}{x_2 - q_2} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = x_1$$

$$q_3 = \lfloor x_3 \rfloor = \lfloor \frac{\sqrt{3}+1}{2} \rfloor = \lfloor 1 + \frac{\sqrt{3}-1}{2} \rfloor = 1 = q_1$$

$$x_4 = \frac{1}{x_3 - q_3} = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \frac{1}{\frac{\sqrt{3}-1}{2}} = \frac{2(\sqrt{3}+1)}{(\sqrt{3}-1)(\sqrt{3}+1)} = \sqrt{3}+1 = x_2$$

$$q_4 = \lfloor x_3 \rfloor = \lfloor \sqrt{3}+1 \rfloor = 2 = q_2$$

$$x_5 = \frac{1}{x_4 - q_4} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = x_3 = x_1$$

$$q_5 = \lfloor x_5 \rfloor = \lfloor x_3 \rfloor = 1 = q_3 = q_1$$

....

....

So, for $n = 1, 2, 3, \cdots$, we have $q_{2n-1} = 1$ and $q_{2n} = 2$. Thus, the *period* of the continued fraction expansion of $\sqrt{3}$ is 2. Therefore, we finally get

$$\boxed{\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}} = [1, \overline{1, 2}].}$$

CFRAC

If we want to factor an integer N, and we have 2 distinct integers x and y for which $x^2 \equiv y^2 \pmod{N}$, then N divides $x^2 - y^2 = (x - y)(x + y)$. This tells us that there is a chance that $\gcd(x - y, N) \neq 1$ or $\gcd(x + y, N) \neq 1$. In particular, if we find many pairs of integers $\{(x_n, y_n)\}^{K}{}_{n=1}$ for which $x^2{}_n \equiv y^2{}_n \pmod{N}$, then there is a high chance that a factor of N can be obtained by computing $\gcd(x_n - y_n, N)$ and $\gcd(x_n + y_n, N)$ for all $1 \leq n \leq k$. We now need a method of generating our good pairs of integers x and y.

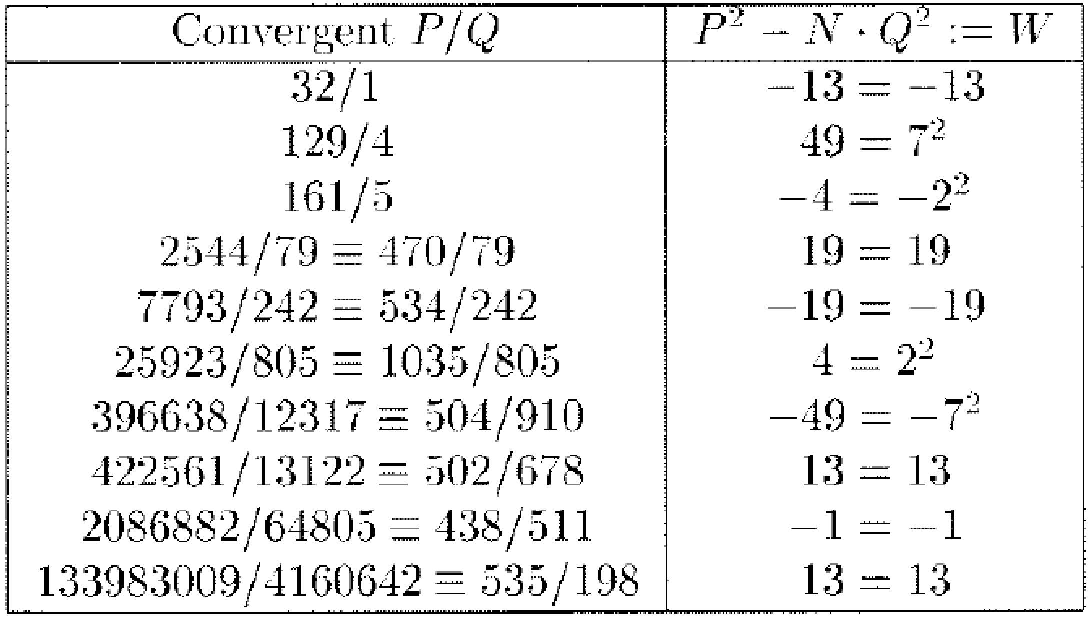
CFRAC

We will illustrate finding x and y with an example: Let n be 1037.

Then we need to find continuous fraction of √1037 which gives us $\sqrt{1037} = [32, \overline{4, 1, 15, 3, 3, 15, 1, 4, 64}]$

Then we must find the continued approximations for those, i.e., Convergent P/Q and find a W using the formula $P^2 - N.Q^2 = W^2$.

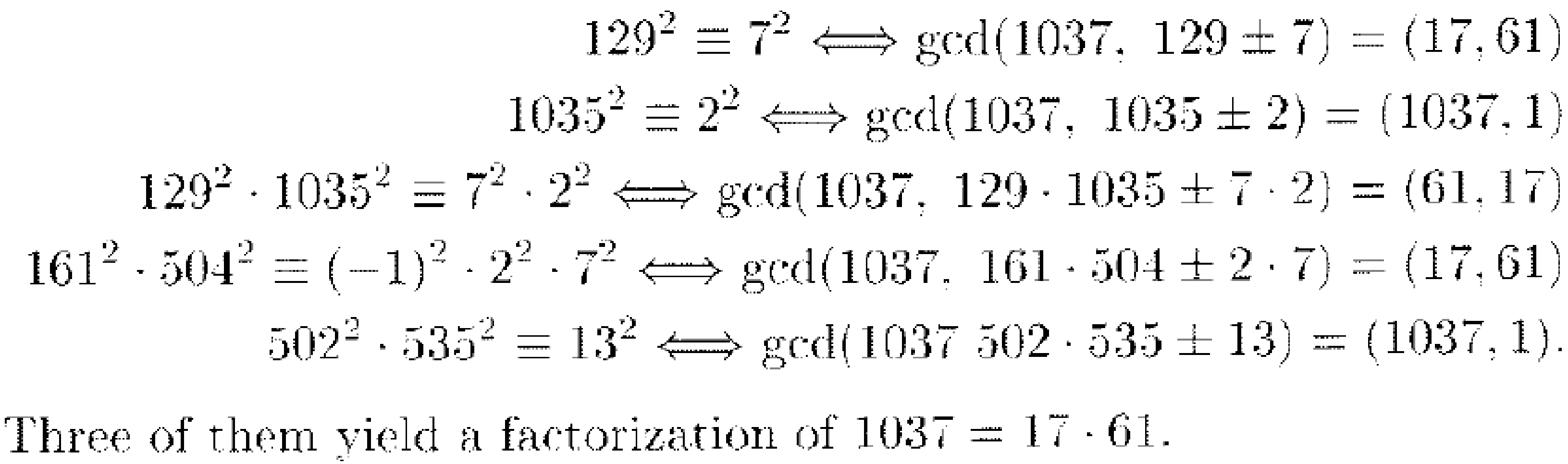
$$\sqrt{1037} = 32 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{15 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{15 \cdots}}}}}}$$



Convergent P/Q	$P^2 - N \cdot Q^2 := W$
$32/1$	$-13 = -13$
$129/4$	$49 = 7^2$
$161/5$	$-4 = -2^2$
$2544/79 \equiv 470/79$	$19 = 19$
$7793/242 \equiv 534/242$	$-19 = -19$
$25923/805 \equiv 1035/805$	$4 = 2^2$
$396638/12317 \equiv 504/910$	$-49 = -7^2$
$422561/13122 \equiv 502/678$	$13 = 13$
$2086882/64805 \equiv 438/511$	$-1 = -1$
$133983009/4160642 \equiv 535/198$	$13 = 13$

CFRAC

Now we search for squares on both sides . Either just by a single congruence or by a combination (i.e ., multiplying together) of several congruences. Once we find squares and it satisfies the condition $P^2 = W^2 \bmod N$.
The two factors can be obtained by taking gcd(N, P-W) and gcd(N,P+W).



$$129^2 \equiv 7^2 \iff \gcd(1037,\ 129 \pm 7) = (17, 61)$$
$$1035^2 \equiv 2^2 \iff \gcd(1037,\ 1035 \pm 2) = (1037, 1)$$
$$129^2 \cdot 1035^2 \equiv 7^2 \cdot 2^2 \iff \gcd(1037,\ 129 \cdot 1035 \pm 7 \cdot 2) = (61, 17)$$
$$161^2 \cdot 504^2 \equiv (-1)^2 \cdot 2^2 \cdot 7^2 \iff \gcd(1037,\ 161 \cdot 504 \pm 2 \cdot 7) = (17, 61)$$
$$502^2 \cdot 535^2 \equiv 13^2 \iff \gcd(1037\ 502 \cdot 535 \pm 13) = (1037, 1).$$

Three of them yield a factorization of $1037 = 17 \cdot 61$.

THANK YOU