Prime Numbers Classification and Composite Numbers Factorization

V. A. Meshkoff
Evpatoria, Republic Crimea, Russian Federation

Abstract On the ground of Prime Numbers Classification it is generalized approach to Composite Numbers Factorization presented. The resulting task goes to the different Diophantine equations reducing. Some methods of reducing and its practical application, in particular for Fermat numbers, are demonstrated.

Keywords Classification, Factorization, Diophantine Equations, Prime Numbers, Fermat Numbers, Generalized Approach

1. Introduction
In simplest presentation the task of the natural numbers factorization determinate as the nontrivial problem of decision for equations in positive numbers

\[ X \cdot Y = N, \quad X, Y > 1 \quad (1) \]

Till present time we have not generalized algebraic methods for those equations, but we have some calculating algorithms for determination all prime components of number N (look [1, 3] and its references). As N rise very big, the calculating problem is growing very hard even for contemporary computing techniques. That situation is remained for numbers sequences, defined algebraic formulas, as Fermat numbers, Mersenne numbers and etc..

As far back Gauss remarked, «… that problem, how to discriminate composite numbers from primes and decompose first’s on its prime components belong to the whole arithmetic major problems» [2, p. 496]. Since then on, beside way proposed by Gauss, it was found many algorithms, for that goal intended. There we will consider only second problem – composite numbers factorization. Present state and achievements at that field is reviewed, for example, in [1, 3], and it connected with algorithmic theory of numbers and computers programming. Though with hard efforts it was attained decomposing on factors very big numbers, generalized theory of factorization doesn’t exist, and we may only talk about phenomenological and particular methods.

In that article the problem of factorization examined on the basis of the prime numbers classification [4]. It permits to reduce factorization to decision of sufficiently simple Diophantine equations.

2. Two Prime Numbers Products Classification
According to classification, presented in [4, p. 37], beside some first, all prime numbers have the linear form

\[ p_i = 24m + r_i, \quad r_i = \{1, 5, 7, 11, 13, 17, 19, 23\}, \quad m \geq 0. \]

We may compose all its products, calculate

\[ p_i p_j (\text{Mod}24) = r_i r_j (\text{Mod}24) \]

and collect results in Table 1.

From Table 1 it is follow, that odd composite numbers have the same linear form of \( \text{Mod}24 \) as prime numbers. So in general the problem of factorization we may to solve as the problem of factorization for two prime numbers products. If in result one of components will be composite, then to it we may to apply the same approach.
3. Factorization as Diophantine Equations Decision

Proposed approach we may demonstrate on simplest examples. For comparing with present methods we take, as example, composite number 45113, which used in [1, pp. 150-168] for discussion of different factorization algorithms.

We compute \( 45113 \equiv 17 \mod(24) \). Then from Table 1, we find 4 possible variants for that composite number: \((r_i, r_j) = (1,17), (5,13), (7,23), (11,19)\). If we have not any additional information, then we must examine all 4 equations, that follows from possible presentations composite number. It is expediently to solve those equations in parallels, that possible diminish computations and permit to escape for proving absence of decision, as for big numbers it may be not simple problem. Then we easy writing out uniformity equations and find out the simple decision of one of its. For other equations that determines the absence of decisions too.

For variant \((1, 17)\) we have after obvious transformations

\[
(24x+1)(24y +17)=45113, \quad 24xy+17x+y=1879=78 \cdot 24+7, \\
17x+y=24s+7, \quad xy+s=78
\]  

(1)

Then we make further transformations and substitutions

\[
17x+y=24s+7, \quad 24s-17x=y-7, \quad s=5(y-7)+17h, \quad x=7(y-7)+24h\]  

(2)

Under conditions \( x>0, y>0 \) and if we substitute its presentations from (2) to last formulae from (1), then we may to see, that have not decision if \( h>0 \). So for \( h<0 \) we have to change sign \( h \) in (2) on minus

\[
s=5(y-7)-17h, \quad x=7(y-7)-24h>0, \quad y-7=4h+a, \quad s=3h+5a, \quad x=4h+7a
\]  

(3)

After substitution formulas for \( x, y, s \) from (3) to last formulae from (1) we have equation with positive unknowns

\[
(4h+a+7)(4h+7a)+3h+5a=78
\]  

(4)

We leave that equation for the time, analogically examine other and present it briefly.

For variant \((5, 13)\) it is

\[
(24x+5)(24y +13)=45113, \quad 24xy+13x+y=1877=78 \cdot 24+5, \\
13x+5(y-1)=24s, \quad 24s-13x=5(y-1), \quad s=4(y-1)+13h, \quad x=7(y-1)+24h>0, \quad h<0
\]  

(5)

For variant \((11, 19)\) it is

\[
(24x+11)(24y +19)=45113, \quad 24xy+19x+11y=1871=78 \cdot 24-1, \\
19x+11y+1=24s, 19(x-4)+11(y+7)=24s, 24s-19(x-4)=11(y+7), \\
s=4(y+7)+19h, \quad x-4=5(y+7)+24h, \quad h<0 \Rightarrow h \Rightarrow -h
\]  

(6)
For variant \((7, 23)\) it is

\[
(24x+7)(24y +23)=45113, \quad 24xy+23x+7y=1873=7\cdot 24+1,
23x+7y-1=24s, \quad 23(x-4)+7(y+13)=24s, \quad 24s-23(x-4)=7(y+13),
\]

\[
s=7(y+13)+23h, \quad x-4=7(y+13)+24h, \quad h<0, \quad h \Rightarrow -h \rightarrow
y=4h+a-13, \quad s=5h+7a, \quad x=4h+7a+4, \quad xy+s=78,(4h+7a+4)(4h+a-13)+5h+7a=78
\]

In result from variant \((5, 13)\) it is easy to have factorization

\[
a=0, \quad h=2, \quad x=8, \quad y=9, \quad 45113=197 \cdot 229
\]

4. Factorization and Diophantine Equations Methods of Decision

Then we examine more complex problem, which Shanks solved with his specially developed algorithm and program for simplest computer or programming calculator [5]. The example that Shanks examine \(N=13290059\), our methods may to solve with aid of ‘pencil and paper’. 

We find \(N \mod 24=11\). Then from Table 1 we find four possible variants for that composite number: \((r_1, r_2) = (1, 11), (5, 7), (13, 23), (17, 19)\).

We write out four initial equations, as we have not any information for some variants. The result is

\[
1) \quad (24x+1)(24y +11)=N, \quad 24xy+11x+y=553752=23073 \cdot 24 \rightarrow
2) \quad (24x+5)(24y +7)=N, \quad 24xy+7x+5y=553751=23073 \cdot 24-1 \rightarrow
3) \quad (24x+13)(24y +23)=N, \quad 24xy+23x+13y=553740=46145 \cdot 12=23072 \cdot 24+12
4) \quad (24x+17)(24y +19)=N, \quad 24xy+19x+17y=553739=23072 \cdot 24+11
\]

Simpler it is presentations of 1st and 3rd variants, then we continue its solving 
For variant \((1, 11)\) it is

\[
11x+y=24s, \quad 24s-11x=23073 \cdot 24 → \quad s=6y-11h, x=13y-24h,
y=2h+a, s=h+6a, x=2h+13a, \quad xy+s=23073 = (2h+a)(2h+13a)+h+6a
\]

For variant \((13, 23)\) it is

\[
23x+13y=24s+12, \quad x=x_1 +1, \quad y = y_1 +1, \quad s=s_1+1, \quad 23x_1 +13y_1 =24s_1,
24s_1-23x_1 =13y_1 \rightarrow s_1=13y_1-23h, x_1=13y_1-24h, y_1=2h+a,
y=2h+a+1, \quad s=3h+13a+1, \quad x=2h+13a+1,
xy+s=23072 = (2h+a+1)(2h+13a+1)+3h+13a+1
\]

Then we present \((11)\) as

\[
4h^2+28ah+7h+13a^2+27a=23070, \quad 4h^2 + h(28a+7)-23070+27a +13a^2 = 0
\]

If that equation has decision in positive whole numbers, then its determinant will be quadrate, so 

\[
D_h=(28a+7)^2 - 4 \cdot 4(-23070+27a +13a^2) = 369169 - 40a + 576a^2 = X^2
\]

Last presentation we may to transform with aid of substitutions and find decision 

\[
- 40a+576a^2 = X^2-369169 > 0, \quad X=607+b, \quad - 40a+576a^2 = 2 \cdot 607b+b^2-720,
b = 8b_1, \quad - 5a + 72a^2 + 90 = 2 \cdot 607b_1+8b_1^2, \quad a=2a_1,
- 5a_1 + 144a_1^2 + 45 = 607b_1+4b_1^2, \quad a_1=2, \quad b_1=1, \quad a=4
\]

That value we substitute in equation \((12)\) and solve it as equation with one unknown quantity
4h^2 + h(28a+7)-23070+27a +13a^2 = 0, a=4, 4h^2 +119h-22754=0, h=62 \quad (15)

From formulas (11) we have factorization

\begin{align*}
y &= 2h+a+1, \quad s=3h+13a+1, \quad x=2h+13a+1, \quad a=4, \quad b=62, \quad y=129, \quad x=177, \\
(24x+13)(24y +23) &= (24 \cdot 177+13)(24 \cdot 129 +23) = 4261 \cdot 3119 = 13290059 \\
\end{align*} \quad (16)

Another method for that factorization is useful too, if \( x, \ y \) are sufficiently close numbers. Then it’s sufficiently close to estimation

\[ x \equiv y, \quad X \approx (xy)^{1/2}, \quad X \approx N^{1/2} / 24 = 13290059^{1/2} / 24 = 151.898 \quad (17) \]

With that estimation we may to write out another initial equation for \( N \)

\[ (24(144+x)+13)(24(144+y)+23)=13290059, \quad 3479 \ x + 3469 \ y + 24 \ x \ y = 50892 \quad (18) \]

Continue to transform we have

\[ -12 \cdot 4241 + 24 \cdot 144(x+y) +23x +13y+24xy =0, \quad x+y=z, \]

\[ -12 \cdot 4241 + 24 \cdot 144z+10x+13z+24(zx-x^2) = 0, \]

\[ 10x+13z=12w, \quad 2 \cdot 144z+2(zx-x^2)+w=4241 \]

Then we find decisions for linear equation from (19) and use it for subsequent substitutions

\[ 12w-13z=10x \rightarrow w=3x-13h, \quad z=2x-12h, \]

\[ x=7k+a, \quad z=2k+2a, \quad w=8k+3a \]

The last formulas are substituted in last equation of (19) and give presentation that have simple decision for first equation of (18)

\[ 579a+2a^2+584k+4ak - 70k^2 = 4241, \quad a=2a, +1, \]

\[ 583a+4a^2+294k+4a, k - 35k^2 = 1830, \quad a_i = 2, k=4, \quad a_5=5, \]

\[ x=7k+a=33, \quad z=x+y=2k+2a=18, \quad y=z-x=15 \quad (21) \]

Thus, in that way practically with «pencil and paper» calculations we may to get number factorization, which Shanks solved with skillful algorithms and computer program [5]. To our mind if such mathematicians as Fermat, Gauss, Euler and another classics of numbers theory were known about presented here approach, they were able even some centuries ago to solve similar problems of number factorization. In principle, our methods give decision of first problem as formulated by Gauss. If we use four equations for factorization like in (9) to prime number, so we will not get components as for composite number. It is proving for prime.

\section*{5. Fermat Numbers Factorization}

One of old classic problem is factorization of Fermat numbers, which have presentation

\[ F_n = 2^{2^n} + 1, \quad n = 1, 2... \quad (22) \]

In work [4, p. 38] it was come in sight that components of composite Fermat numbers must be only prime numbers \( 24m+1 \) in some quantity and prime numbers \( 24m+17 \) in odd quantity. So in that case the problem of factorization is simplified, as for decision it is enough to examine only one equation.

Besides that, it is another property of the components, which we may to use: components of composite \( F_n \) have presentation \( 2^{n+2} k + 1 \) [1, p. 47]. That information permits to get new formulas for components.

Then for \( F_5 \) we have for first component presentation

\[ 2^7k+1 = 24m+1, \quad 2^7k = 24m', \quad k=3m, \quad m'=2^4m, \quad f_{5j} = 384m+1 \quad (23) \]
For another component analogically we have
\[ 2^k + 1 = 24p + 17, \quad 2^k - 24p = 16, \quad 16k - 3p = 2, \]
\[ k = 2 + 3p, \quad p = 10 + 16p, \quad f_{517} = 384p + 257 \]  
(24)

Thus we may to write out initial equation for \( F_5 \) factorization
\[ (384m + 1)(384p + 257) = 2^{32} + 1, \]
\[ 384mp + 257m + p = 2(2^{24} - 1)/3 = 11184810 = 384 \cdot 29127 + 42, \]
\[ 257m + p = 42 + 384s \rightarrow mp + s = 29127 \]  
(25)

We find the decision for last linear equation from (25)
\[ 257m - 384s = 42 - p, \quad m = 127(p - 42) + 384t, \quad s = 85(p - 42) + 257t \]  
(26)

Substitution this to last equation from (25) gives
\[ p(127(p - 42) + 384t) + 85(p - 42) + 257t = 29127, \]
\[ -5249p + 127p^2 + 257t + 384pt = 32697 \]  
(27)

We use then simple identity and get final equation
\[ 127 = 384 - 257, \quad 5249 = 13 \cdot 384 + 257, \]
\[ 384p(p + t - 13) + 257(t - p^2) = 32954 \]  
(28)

It is easy to find analogical presentation for right side (28) and end decision
\[ 384a = 32954 \pmod{257}, \quad 384a = 58 \pmod{257}, \quad a = 47, \]
\[ 32954 = 384 \cdot 47 + 257 \cdot 58, \quad p(t + t - 13) = 47, \quad t - p^2 = 58, \]
\[ p = 1, \quad t = 59, \quad m = 127(p - 42) + 384t = 17449, \]
\[ F_5 = (384m + 1)(384p + 257) = (384 \cdot 17449 + 1)(384 + 257) = 6700417 \cdot 641 \]  
(29)

Of course, the factorization search in that case is relieved, as the result is known. But our aim is to demonstrate process of decision with elementary methods, which do not used since Fermat time to present. Fermat error suggested (in 1640-1654) that all numbers \( F_n \) are primes. Euler since century found component 641, that divide \( F_5 \). Next factorization for \( F_6 \) was found at 1880 [6, pp. 375-380]. Those give us some foundations to suggest: if the way demonstrated above may be known Fermat and his colleagues, the development of factorization methods went another and more rapid road.

6. Fermat Numbers Factorization (Continuation)

The problem \( F_6 \) factorization is harder in sense of calculations. In general the complicate situation with Fermat numbers consist in its rapid increasing and even for best method of decision get up straight technical complexities in the field of «big numbers». The case with \( F_6 \) is transitional as its factorization was found «after several months’ labor» [6, p. 377]. Factorization for \( F_5 \) occurred at 1975 in era of computers, so there we restrict that article only of case \( F_6 \).

Initial equation we get after transformation, analogous (23-25)
\[ F_6 = 2^{64} + 1 = (2^8k_1 + 1)(2^8k_2 + 1) = (24a + 1)(24b + 17), \quad k_1 = 3n, \quad a = 2^5, \]
\[ 24b + 17 = 2^6k_2 + 1, \quad 2^6k_2 - 3b = 2, \quad k_2 = 1 + 3m, \quad b = 10 + 2^5m, \]
\[ (768n + 1)(768m + 257) = 2^{64} + 1, \quad 768mn + 257n + m = (2^{56} - 1)/3 =
\[ 24019198012642645 = 768 \cdot 31274997412295 + 85 \]  
(30)

Further we go another way
\[ 257n + m = 85 + 768s, \quad mn + s = M = 31274997412295 = 768 \cdot 40722652880 + 455, \]
\[ m = 85 + 768s - 257n, \quad s = k + n, \quad m = 85 + 768k + 511n \]

Substitution those presentations give us
\[ mn + s = 768nk + 511n^2 + 86n + k = M, \]
\[ 511n^2 + 86n + k = 768s_i + 455, \quad nk + s_i = 40722652880 \]

We take transformations with parameter \( A \) – whole positive number
\[ s_i = n^2 + A n + r, \quad k = 257n^2 + (A - 86)n + 768r + 455 \]

After further substitutions (33) to last formulae (32) we have Diophantine equation third degree, where \( A \) is variable parameter
\[ 257n^3 + (768A - 85)n^2 + (455 + A)n + 768nr + r = 40722652880 \]

That equation has transformation to
\[ 257n^3 - 85n^2 + 455n + (768n + 1)(An + r) = 40722652880 \]

As \( n > 0 \), so if whole number \( A > 0 \) and \( r > 0 \) there is some value \( \tilde{A} \) when exist minimum \( n > r > 0 \). But it is known, that equation (34) has one decision in whole positive numbers \( (n, r_A) \), \( r_A = An + r = \text{const.} \). If \( A = 0 \), then \( r_A = r_0 \). When we will to increase \( A \) to \( \tilde{A} \), \( r \) will be to decrease to \( r_\tilde{A} = \min r \). If then we take \( A = \tilde{A} + 1 \), \( r_A = n(\tilde{A} + 1) + r_{\tilde{A} + 1} = n\tilde{A} + r_\tilde{A} \), \( r_{\tilde{A} + 1} = r_\tilde{A} - n < 0 \).

Then for all \( A > \tilde{A}, r < 0 \). So it is monotone dependence, and for \( r = r_A = \min r \) there is local positive minimum, and for \( r = r_{\tilde{A} + 1} < 0 \) there is local maximum. From (35) we get
\[ r = \frac{40722652880 - (257n^3 - 85n^2 + 455n)}{768n + 1} - An \]

We come to problem of two-dimension searching on field of positive natural numbers for whole local extremum of \( r \) near value \( r = 0 \) with simplifying conditions \( A \geq 0, n > r > 0 \). There we present decision results omit details:
\[ \tilde{A} = 296, \quad n = 357, \quad r_A = 245; \quad \tilde{A} + 1 = 297, \quad n = 357, \quad r_{\tilde{A} + 1} = -112 \]

We must note that problems (35) and (36) now it is easy to decide with computer program, in particular with Mathematica of Wolfram Research. \textit{Reduce} program decide (35) and (36) for all values \( A \), and for negative values too, as when \( A < 0 \) decrease, \( r \) increase and \( r = r_0 + |A| n \).

Now it is great amount of studies, guides and manuals on Diophantine equations, but as we may to see, the approach to factorization presented here was unknown, so corresponding equations have no attention of researchers. The equations of second degree is mentioned in [6, pp. 412-417], as with use of classical methods lead to problem of factorization, but another methods did not studied. Diophantine equation third degree, similar to (34-35) also did not study, but may be classified as inhomogeneous Thue equation \( f(x, y) = m \) [7]. There authors assert, that their paper «gives in details a practical general method for explicit determination of all solutions of any Thue equation». But now it is unknown Thue equations application for factorization problem.

With another side, elliptic curves third degree application, i.e. Thue equations, is known in factorization algorithms [1, p. 83; 3, p. 319]. However, those connections are outside present article and demands serious researching.
7. Conclusions

For our mind, we presented new approach to factorization problem. It is surprising, why it was unknown some centuries ago, as demand highly elementary mathematical means and notions. Here we in the main examined examples, that may be decided with «pencil and paper». Diophantine equations, ensuing from presented concrete tasks and its methods of decision are not exhaustive. It needs further development and researching.

Now it is known private effective algorithms and computer programs for factorizations in the wide diapason to big numbers. In that sense the list of references has not fullness and is biased to aim of article. For other well-known material on Factorization we refer to MathWorld – A Wolfram Web Resource.

There is whole factorization for \( F_{11} \) and all previous Fermat numbers. But \( F_{12} \) is factored incomplete and composite fragment of it has 1133 decimal digits. So it is interesting whether presented here Diophantine equations methods will be effective for big number problems. However, that needs serious special studying with high quality programming and technical means, and so exceed the limits of present article, as its main aim is only to demonstrate opportunity of new generalized approach for factorization.

REFERENCES

[1] Sh.T. Ishmukhametov. Methods for the factorization of natural numbers: a tutorial. Kazan University Publ., Kazan, 2011. (Russian edition: Kazan, 2011).

[2] K.F. Gauss. Works on number theory. Publishing House of the Academy of Sciences, Moscow, 1959. (Russian edition: Moskow, 1959).

[3] R. Crandall, C. Pomerance. Prime numbers. A computational perspective. Springer, New York, 2005.

[4] V. Meshkoff. Prime Numbers Classification with Linear and Quadratic Forms. Universal Journal of Applied Mathematics 3(3): 35-39, 2015

[5] D. Shanks. SQUFOF Notes. Manuscript. Available at: David Joyner and Stephen McMath. http://cadigweb.ev.usna.edu/~wdj/mcmath/

[6] L.E. Dickson. History of the theory of numbers. Vol. I. Chelsea Publishing Company, New York, 1952.

[7] N. Tzanakis, B.M.M. de Weger On the practical solutions of the Thue equation. Journal of Number Theory 31, 99-132 (1989)