Fermat's method of factorisation

PETER SHIU

1. *Introduction*

On 7 April 1643, Fermat wrote the following intriguing letter (see [1]) to Mersenne:

> You ask whether the number 100895598169 is prime or not, and for a method to decide, within a day, whether it is prime or composite. To this question I answer that the number is composite, being the product of 898423 and 112303, which are primes. I remain always, reverend Father, your very humble and very affectionate servant. Fermat.

It seems likely that Fermat had claimed that he could factorise numbers up to about 10^{11}, and that Mersenne then constructed the two primes in the letter and sent the product as a challenge to him. No one knows how Fermat managed to find the factors 'within a day'.

Fermat disclosed partially his method of factorisation, which applies to any odd composite number N. One tries to find integers A and B such that

$$N = A^2 - B^2,$$

so that two factors for N are given by

$$P = A - B \qquad \text{and} \qquad Q = A + B.$$

The time, or effort, involved is spent almost entirely on the square test, which amounts to checking whether the square-root of a number is an integer. The test is applied to $A^2 - N$ with successive values of $A \geqslant \sqrt{N}$, so that B^2 is delivered, but the method is viable only when there is success with A near $\sqrt{N}$.

For Mersenne's challenge number N, the square test is applied with every $A \geqslant \sqrt{N} > 317640$, until success comes at $A = 505363$, so that $N = A^2 - B^2$ with $B = 393060$, yielding the factors P and Q in Fermat's letter. Obviously Fermat did not apply 187723 square tests, so he must have had some tricks up his sleeve. It is our speculation that he knew the enhancement of his method we consider here.

2. *An enhancement of the method*

If $x^2 - y^2 \equiv 1 \pmod 4$ then x has to be odd, and if $x^2 - y^2 \equiv -1 \pmod 4$ then x has to be even. Similarly, if $x^2 - y^2 \equiv 2 \pmod 3$ then x has to be a multiple of 3. Such observations lead us to an enhancement of Fermat's method of factorisation because, in general, we have the following proposition, which can be deduced from a well-known result on difference sets associated with quadratic residues (see, for example, [2]).

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

Proposition: For an odd prime p not dividing d, the number of solutions in $x \pmod p$ to the congruence $x^2 - y^2 \equiv d \pmod p$ is $(p + \theta)/2$, where $|\theta| = 1,3$; if $p \equiv 3 \pmod 4$ then $|\theta| = 1$.

Take, for example, $p = 19$, $d = 18$. Then $x^2 - y^2 \equiv 18 \pmod{19}$ has the nine solutions for $x \equiv 0, \pm2, \pm4, \pm5, \pm9$ corresponding to $x^2 \equiv 0, 4, 16, 6, 5$; $y^2 \equiv 1, 5, 17, 7, 6$.

Now, in Fermat's method, for each odd prime p not dividing $N = A^2 - B^2$, there are, according to the proposition, only about $p/2$ admissible values for $A \pmod p$. Applying the argument to n odd primes, the process should reduce the number of square tests by a factor of about 2^n. More specifically, let p_i be the chosen odd primes, $D = \prod p_i$, and a_i be the corresponding possible values for $A \pmod{p_i}$. Then, by the Chinese remainder theorem (CRT), each vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ delivers a solution to the system of simultaneous congruences

$$A \equiv a_i \pmod{p_i}, \qquad i = 1, 2, \ldots, n,$$

in the form $A \equiv r \pmod D$, where $0 \leqslant r < D$. We may then write

$$A = kD + r, \qquad k = 0, 1, 2, \ldots, \qquad r \in \mathcal{R},$$

where $\mathcal{R}$ is a set of possible remainders determined from the CRT. For each k, we need only perform the square test on $|\mathcal{R}| \approx D/2^n$ values of $A^2 - N$.

Roughly speaking, the reduction in the number of square tests is paid for by the repeated use of the CRT. The enhancement provides an interesting exercise in computer programming because, in common with many interesting problems in computational number theory (such as the counting of prime numbers) there is a trade off between the time used and the amount of memory space being available in the search for the solution.

3. *An example*

In his *Disquisitiones Arithmeticae*, Gauss chose $314159265 = 3^2 \cdot 5 \cdot 7N$, where

$$N = 997331,$$

to illustrate several of his factorisation methods; see §§329-334 in [3]. We now take this N as our first example. The solutions to $A \pmod p$ corresponding to $N \pmod p$ are given in the following table—note the agreement with the proposition.

p	$N \pmod p$	$A^2 \pmod p$	$A \pmod p$
2	3 (mod 4)	0 (mod 4)	0
3	2	0	0
5	1	0,1	0, ±1
7	6	0,1	0, ±1
11	5	3, 5, 9	±3, ±4, ±5

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

Thus, we know that $6 \mid A$, so that we need only consider $p = 5, 7, 11$, with the corresponding vector $\mathbf{a} = (a, b, c)$, where $a, b = 0, \pm 1$, and $c = \pm 3, \pm 4, \pm 5$. The set $\mathcal{R}$ can now be determined from the CRT.

Ignoring $p = 11$ for the moment, so that $\mathbf{a} = (a, b)$, and there are 9 systems of two simultaneous congruences $A \equiv x \pmod{p}$, where $(p, x) = (5, a), (7, b)$. Together with $A \equiv 0 \pmod 6$, the CRT then delivers

$$A = kD + r, \quad D = 2\cdot 3\cdot 5\cdot 7 = 210, \quad r \in \mathcal{R} = \{0,6,36,84,90,120,126,174,210\}.$$

The square test is now applied to $A^2 - N = (210k + r)^2 - 997331$, starting with $k = \lceil \sqrt{997331}/210 \rceil = 5$. Thus, for each $k \geqslant 5$, and $r \in \mathcal{R}$, we test the number until the square 3863^2 emerges with $k = 19$, $r = 0$, delivering

$$A = 3990, \qquad B = 3863, \qquad P = 127, \qquad Q = 7853;$$

the number of tests being applied is $(18 - 4) \times 9 + 1 = 127$.

If we include $p = 11$ then $D = 2310$, and there are now 54 systems of 3 simultaneous congruences, but the number of square tests should be reduced down to about 70 according to our prediction. Thus, using the CRT, we find that

$\mathcal{R}$ = {6, 36, 84, 126, 204, 216, 246, 294, 300, 336, 414, 426, 456, 510, 546, 624, 630, 666, 720, 756, 840, 876, 930, 960, 1050, 1086, 1140, 1170, 1224, 1260, 1350, 1380, 1434, 1470, 1554, 1590, 1644, 1680, 1686, 1764, 1800, 1854, 1884, 1896, 1974, 2010, 2016, 2064, 2094, 2106, 2184, 2226, 2274, 2304};

the square test again delivers $A = 3990$, at $k = 1$, $r = 1680$. When $k = 0$ we need to have $r \geqslant \lceil \sqrt{997331} \rceil = 999$, so that the number of tests is $30 + 38 = 68$.

Without the enhancement, the required number of square tests is about 3000. We note that $A \equiv 0 \pmod{2, 3, 5, 7}$, but this is not contrived luck. As we already noted in x^2, we always have a 'free-ride' for $p = 2$, and a further one for $p = 3$ if $N \equiv 2 \pmod 3$; also $35 \mid A$ is used only as one of 9 possibilities in our search. In any case, we chose the example by following Gauss!

4. *Fermat's factorisation of* $N = 100895598169$

We speculate that Fermat was well aware of our enhancement, and he would even have the results of frequently used calculations tabulated. Thus, for each odd prime $p < 20$, say, and $d \not\equiv 0 \pmod p$, Fermat would have constructed tables for all the possible values of $A \pmod p$ satisfying $A^2 - B^2 \equiv d \pmod p$. On receiving the challenge $N = 100895598169$ from Mersenne, he could quickly jot down the following:

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

p	$N \pmod p$	$A^2 \pmod p$	$A \pmod p$
2	1 (mod 4)	1 (mod 4)	1
3	1	1	±1
5	4	0, 4	0, ±2
7	2	4	±2
11	3	1, 3, 4	±1, ±2, ±5
13	2	1, 3, 12	±1, ±3, ±5
17	7	8, 9, 15, 16	±3, ±4, ±5, ±7
19	9	1, 6, 7, 9, 16	±1, ±3, ±4, ±5, ±8

The product of the primes up to 17 is $510510 > \sqrt{N}$, and we know that A is odd. From the table, there are $2 \times 3 \times 2 \times 6 \times 6 \times 8 = 3456$ vectors $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$ corresponding to $3 \leqslant p \leqslant 17$, so that there are 3456 systems of 6 simultaneous congruences to be solved.

Faced with such a daunting task it is likely that Fermat would first consider $a_1 = a_4 = a_5 = 1$, giving $A \equiv 1 \pmod{858}$, so that there are only $3 \times 2 \times 8 = 48$ systems of 3 simultaneous congruences corresponding to $\mathbf{a} = (1, a_2, a_3, 1, 1, a_6)$ to solve. For each of the 48 possible solutions with $A \geqslant \sqrt{N} > 317640$, he had to check whether $A^2 - N$ is a square. Fermat knew so much about squares that he could easily dismiss numbers of this size, or knew that he had found a solution. Thus, well 'within a day', he would have found that $\mathbf{a} = (1, -2, -2, 1, 1, 4)$, corresponding to $A = 505363$, delivers the factors for N in his letter.

Indeed, noting that $A \equiv 1 \pmod{19}$ is admissible, whereas $A \not\equiv 1 \pmod{17}$, Fermat might have taken the former, and ignore $p = 17$ altogether. If he did then he only had 6 systems to deal with, but that will be more than speculating.

5. *The factorisation of* $F_5 = 2^{2^5} + 1$

Presumably Fermat was so convinced that 'his' number

$$N = F_5 = 2^{2^5} + 1 = 4294967297$$

was prime that he made no serious effort to factorise it. The number was factorised by Euler in 1732, using his discovery that a prime factor p of F_5 has to satisfy $p \equiv 1 \pmod{128}$; apparently Fermat might have known this already, but he did not make use of it. Indeed there are several simple ways to discover the prime divisor 641 of F_5; we continue to use Fermat's method for illustration.

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

If $P \equiv 1 \pmod{128}$ then $Q \equiv PQ \equiv N \equiv 1 \pmod{128}$, so that $2A \equiv P + Q \equiv 2 \pmod{128}$, and hence $A \equiv 1 \pmod{64}$. Allowing ourselves to write $p = 64$ we have the table below.

p	$N \pmod p$	$A^2 \pmod p$	$A \pmod p$
64	1 (mod 128)	1 (mod 128)	1
3	2	0	0
5	2	1	±1
7	5	0, 2	0, ±3
11	5	3, 5, 9	±3, ±4, ±5

The first two rows of the table shows that $A \equiv 129 \pmod{192}$. For $p = 3$, 5, 7 there are now $2\cdot3\cdot6 = 36$ vectors $\mathbf{a} = (a, b, c)$ to deal with. Setting $D = 192\cdot5\cdot7\cdot11 = 73920$, the CRT then delivers the 36 numbers in the set

$$\mathcal{R} = \{129,\ 1281,\ 4161,\ \ldots,\ 21249, \underline{24129},\ 25281, \ldots, 68481, 71361, 72321\}.$$

With $A = kD + r$, $r \in \mathcal{R}$, the square test then shows that $A^2 - N = 33498882$ when $A = 3350529$ at $k = 45$, with $r = 24129$, the 15th member of $\mathcal{R}$ according to size, which corresponds to $\mathbf{a} = (-1,\ 0,\ -5)$. The factorisation $P = 641$, $Q = 6700417$ is found with fewer than $46 \times 36 = 1656$ square tests.

6. *The factors for* $F_6 = 2^{2^6} + 1$

It has to be said that the method becomes extremely tedious when N is no longer small, and perhaps hopelessly so when $N > 10^{30}$, say. We illustrate the difficulties involved by considering the sixth Fermat number

$$N = F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 18446744073709551617,$$

which was factorised by F. Landry in 1880, 'after several months of work' at the age of 82. Meanwhile Euler's discovery had been generalised by E. Lucas to $p \equiv 1 \pmod{2^{n+2}}$ for prime divisors of F_n. We can then use $A \equiv 1 \pmod{128}$, together with the entries in the following table; we also note that $\sqrt{N} \approx 2^{32} \approx 4 \times 10^9$.

p	$N \pmod p$	$A^2 \pmod p$	$A \pmod p$
128	1	1	Lucas: 1
3	2	0	0
5	2	1	±1
7	3	0, 4	0, ±2
11	6	0, 4, 9	0, ±2, ±3

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

13	4	0, 1, 3, 4	0, ±1, ±2, ±4
17	2	0, 1, 2, 4, 15	0, ±1, ±6, ±2, ±7
19	18	0, 4, 5, 6, 16	0, ±2, ±9, ±5, ±4
23	7	0, 2, 8, 9, 13, 16	0, ±5, ±10, ±3, ±6, ±4
29	25	0, 1, 5, 9, 16, 20, 24, 25	0, ±1, ±11, ±3, ±4, ±7, ±13, ±5

Excluding $p = 29$ for the moment, we set

$$D = D_{23} = 128\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23 = 14277943680,$$

and $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ corresponding to $5 \leqslant p \leqslant 23$. We then require

$$|\mathscr{R}| = |\mathscr{R}_{23}| = 2\cdot3\cdot5\cdot7\cdot9^2\cdot11 = 187110$$

stores for the possible remainders. Anyway, with $A = kD + r$, success comes at $k = 2356$ and $r = 1375482369$, the 18110 th member of $\mathscr{R}_{23}$, delivering the factors

$$P = 274177 \qquad \text{and} \qquad Q = 67280421310721,$$

corresponding to

$$A = 33640210792449, \qquad B = 33640210518272.$$

The solution vector is $\mathbf{a} = (-1, 2, -3, 1, -7, -2, 6)$, and the number of square tests is about $2356 \times 187110 \approx 5 \times 10^8$.

The number of square tests can be reduced by including $p = 29$, so that $D_{29} = 414060366720$, but then $|\mathscr{R}_{29}| = 2806650$ may be rather large for a small machine. We can, of course, partition $\mathscr{R}_{29}$ into 15 subsets $\mathscr{R}'$ according to the values of A (mod 29) in the table. In other words, we can run the '$\mathscr{R}_{23}$ program' 15 times corresponding to each of the possible values A (mod 29), with a speed up factor of 1 / 29 for each run. Success comes on the run with $A = 4$ (mod 29), delivering $A = kD_{29} + r$, at $k = 81$ and $r = 101321088129$, the 45832th member of the subset $\mathscr{R}_{29}'$. If we order the possible values for A (mod 29) by size, taking +4 for the sixth run, then the time taken is less than a quarter of that for the successful search using D_{23} and $\mathscr{R}_{23}$.

7. *Some relevant remarks on the method*

What we call our enhancement is well known to the experts on factorisation. Another standard trick is to replace N by aN, where a has a known factorisation, and the method becomes effective if A is close to $\sqrt{aN}$. Indeed, in the 1920s, M. Kraitchik gave a thorough reappraisal of the method, dispensed with the square test, and introduced radical ideas which form the basis of modern factoring algorithms. More information can be found in the interesting article [4].

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press

For the factorisation of $N < 10^{30}$, say, Pollard's ρ-method is probably best. Much has been written about this probabilistic method in various recent texts (see, for example, [5]) so that we need only report here that $N = 997331$, 100895598169, F_5, F_6 can be factorised in 'no time' by the method. More specifically, with our randomly chosen seed $a = 73$ for the quadratic $x^2 + a$ and the randomly chosen starting point $s = 7671$, the factors for N are delivered in fractions of a second on a small machine, with only 13, 42, 14, and 339 iterations, respectively. The number of iterations is, on average, proportional to the square root of the least prime divisor of N.

The substance of the present article comes from my effort in trying to understand the mathematics used in the factorisation of the Mersenne number $M_{67} = 2^{67} - 1$. The factorisation was found by F. N. Cole [6], and the accompanying tale is given in [7].

References

1. Edouard Lucas, *Récreations Mathématiques*, (1894) Note 230. Translation by Luke Welsh accessed December 2014 at http://primes.utm.edu/mersenne/LukeMirror/litlit_068s.htm.
2. Douglas R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer (2004).
3. C. F. Gauss, *Disquisitiones Arithmeticae* (1801); translated by Arthur A. Clarke, Yale University Press (1966).
4. Carl Pomerance, A tale of two sieves, *Notices of the Amer. Math. Soc.* **43** 12 (1996) pp. 1473-1485.
5. Richard Crandall and Carl Pomerance, *Prime numbers*: *a computational perspective* (2nd edn.), Springer (2005).
6. F. N. Cole, On the factoring of large numbers, *Bull. Amer. Math. Soc.*, **10** (3), (1903) pp. 134-137.
7. Peter Shiu, The factorisation of $2^{67} - 1$, *Math. Gaz.* **99** (March 2015) pp. 104-108.

doi: 10.1017/mag.2014.12

PETER SHIU
353 Fulwood Road, Sheffield S10 3BQ
e-mail: *p.shiu@yahoo.co.uk*

https://doi.org/10.1017/mag.2014.12 Published online by Cambridge University Press