and those for which $m = \frac{1}{2}$. With regard to the former of these classes, for example, it may be shown that if an arbitrary function $f(z)$ be expanded in the form

$$f(z) = a_0 W_{1/2,\,0}(z) + a_1 W_{3/2,\,0}(z) + a_2 W_{5/2,\,0}(z) + \cdots,$$

then the coefficients are given by the relation

$$a_n = \frac{1}{(n!)^2} \int_0^\infty f(z)\, W_{n+\frac{1}{2}}(z)\, \frac{dz}{z}.$$

TRINITY COLLEGE, CAMBRIDGE,
July, 1903.

ON THE FACTORING OF LARGE NUMBERS.

BY PROFESSOR F. N. COLE.

(Read before the American Mathematical Society, October 31, 1903.)

1. IN resolving a large number N into its prime factors, a table of quadratic remainders of N can be made to render efficient service in several different ways. For a twenty-two place N, the remainders of the table may be restricted to products of about seventy of the smallest prime numbers available. If, for example, N is always expressed in the form $N = x^2 \pm a$, with variable x and a, the remainders $\mp a$ will contain only those primes of which N is quadratic remainder. By a gradual elimination of common factors from the remainders $\mp a$, we finally obtain a table of remainders not admitting further reduction. Other forms for expressing N, such as $N = 2x^2 \pm b$, are of course often advantageous, according to circumstances. If the final table of remainders consists entirely of the individual primes employed, each with the proper sign + or −, N is undoubtedly a prime number *; in fact a much smaller sequence of prime remainders would suffice to justify this conclusion, the wide range specified above being required only to ensure the success of the preliminary elimination process. If, on the other hand, it is found impossible, on repeated attempt,

* For an interesting discussion of the use of the table of remainders see P. Seelhoff, *Zeitschrift für Mathematik und Physik*, vol. 31 (1886), pp. 166, 174, 306.

to isolate the prime numbers as remainders, there is a strong presumption amounting almost to certainty that N is compound.

By the aid of the quadratic remainders of the table it is now theoretically possible to construct the factors of N synthetically. Occasionally the form of these factors is so far known in advance that it is not an over serious task to sift all possible cases up to several millions. In the sifting process each known quadratic remainder reduces the number of possible factors of N by one-half. Thus, with twenty-four remainders at hand, sixteen million numbers would be reduced to one or two. In the practice a few of the known remainders would be employed to establish linear series $lx + m$ with variable x; the other remainders would then be used to sift the values of x.

If, however, the smallest factor of N has nine or more places, a much more expeditious method is to employ the known quadratic remainders to reduce N to the form

$$x^2 - y^2 = [\tfrac{1}{2}(u + v)]^2 - [\tfrac{1}{2}(u - v)]^2 = uv,$$

the factors u and v being so chosen that their difference $u - v$ is as small as possible. The advantage of this method is the following: If the table of quadratic remainders is constructed solely from resolutions $N = x^2 + a$, u and v are quadratic remainders of every prime remainder r of the table, and as the product $uv = N$ is known, the symmetric function $u + v$ admits at most $\frac{1}{4}(r + 3)$ values, mod r. Every known prime remainder r therefore cuts down the number of possible values of $u + v$ to about *one-fourth* their number. Other limitations on the value of $u + v$ and $u - v$ may also occur to facilitate the process.

2. Next to the Fermat numbers $2^{2^n} + 1$, the numbers of the form $2^p - 1$, where p is a prime, have attracted the greatest attention as regards their resolution into prime factors. Some curious misinformation in regard to these numbers was published by Mersenne in the preface of his Cogitata physico-mathematica (1644).* A table of their prime factors, as far as $2^{59} - 1$, is most easily accessible in Lucas's article: "Théorie des fonctions numériques simplement périodiques," in volume 1 of the *American Journal of Mathematics*.† The smallest factors are given, so far as known, up to $p = 257$, by Lucas on page 375 of his Théorie des nombres, and on the following page

* *Cf.* Lucas, Théorie des nombres, p. 376.

† The table occurs on pp. 239–240 of the volume.

of the same work the author announces that his calculations indicate that $2^{67} - 1$ and $2^{89} - 1$ are compound. It is known that $2^{61} - 1$ is a prime number.* In the article cited above, Lucas presented a brilliant method for ascertaining whether a given number is prime. His computations just mentioned are doubtless based on this method, which however does not furnish the means of actually finding the factors of the number examined.

3. For the number

$$2^{67} - 1 = 147573952589676412927$$

I found the following apparently irreducible quadratic remainders:

$$2, \ -3, \ -7, \ 13, \ -23.53, \ 37, \ 41, \ 61, \ -67, \ -71, \ 23.83, \ 89, \ 97, \ 101, \ -23.113, \ -127, \ 137, \ 23.151, \ -23.157, \ 23.167, \ 173, \ 181, \ 23.191, \ -23.193, \ \cdots.$$

The conclusion was inevitable, especially in view of Lucas's prediction, that $2^{67} - 1$ possessed precisely two prime factors greater than 1.

It is well known that every factor of $2^p - 1$, p being a prime, is of the forms $kp + 1$ and $8l \pm 1$. Every factor of $2^{67} - 1$ is therefore of the forms $536k + 1$, $536l + 135$, which are further specialized to $1608k + 1$ and $1608l + 1207$ by virtue of their common quadratic remainder -3. With the help of the other small prime remainders, fortified by the presumption that -23 and therefore 53, -83, $\cdots$ were non-remainders, I had no difficulty in sifting the first sixteen million natural numbers, but the search proved without result.

Turning then to the resolution

$$2^{67} - 1 = [\tfrac{1}{2}(u + v)]^2 - [\tfrac{1}{2}(u - v)]^2,$$

and noting that $u - v$ is divisible by 3 and 67, I found the following congruences for determining $\frac{1}{2}(u + v)$:

$$\begin{aligned} \tfrac{1}{2}(u + v) &\equiv 671 \pmod{67^2} \equiv 0 \pmod 8 \equiv 1, 4^+ \pmod 5 \\ &\equiv 1, 3^+ \pmod 7 \equiv 0, 1^+, 12 \pmod{13} \\ &\equiv 10, 37, 46^+, 64 \pmod{81}. \end{aligned}$$

* P. Seelhoff, l. c., p. 174. Seelhoff's papers cited above contain several errata, and his proof that $2^{61} - 1$ is a prime number is hardly satisfactory. I have, however, verified the fact by the actual computation of a sequence of prime remainders. The verification has also been made by others; see Weber-Wellstein: Encyclopaedie der Elementar-Mathematik, p. 48.

The cases marked $^+$ give

$$\tfrac{1}{2}(u+v) = 1323536760x + 1160932384.$$

Sifting with 23, 37, 41, 53, 61, I find $x = 287$ remaining. A few further tests suffice to show that the goal is near. And, in fact,

$$287.1323536760 + 1160932384 = 381015982504,$$

and

$$\begin{aligned} 2^{67} - 1 &= 381015982504^2 - 380822274783^2 \\ &= 193707721 \times 761838257287. \end{aligned}$$

COLUMBIA UNIVERSITY,
October, 1903.

NOTE ON THE p-DISCRIMINANT OF ORDINARY LINEAR DIFFERENTIAL EQUATIONS.

BY PROFESSOR ARNOLD EMCH.

(Read before the American Mathematical Society, August 31, 1903.)

IN a fundamental memoir * Darboux has proved that the resultant $g(x, y) = 0$ obtained by the elimination of $p = dy/dx$ between

$$\phi(x, y, p) = 0 \ (1), \quad \text{and} \quad \partial\phi/\partial p \ (2),$$

where ϕ is a polynomial in x, y, p, represents in general the locus of the cusps of the integral curves.†

For this purpose Darboux first proves that the resultant obtained by the elimination of p between

$$\phi(x, y, p) = 0 \ (3), \quad \text{and} \quad \frac{\partial\phi}{\partial x} + p\frac{\partial\phi}{\partial y} = 0 \ (4)$$

represents in general the locus of the points of inflexion of the integral curves.

By purely geometric reasoning, applying the principle of duality, Darboux then concludes that to this theorem corresponds dualistically the theorem in connection with equations (1) and (2) as stated above.

* "Sur les solutions singulières des équations aux derivées ordinaires du premier ordre." *Bull. des Sciences Math. et Astron.*, vol. 4, pp. 158–176 (1873).

† For an analytic proof see Picard's Traité d'Analyse, vol. 3, pp. 529–534.