Determination of certain Primes. By F. W. LAWRENCE.

Received and Read May 13th, 1897.

The method of "factorisation" is that of my paper in the *Quarterly Journal of Mathematics* (No. CXI., 1896), except that, "strips" being not required, all the work is shown directly.

The primes found are:

77,843,839,397,	a factor of	$10^{29}-1$,
182,521,213,001,	„ „	$10^{25}-1$,
1,001,523,179,	„ „	$3^{23}-1$,
12,014,633,		
13,477,969.		

In order to avoid continual reference, I quote here the notation used in my paper, and certain propositions proved there, which will be used in the investigation.

Notation.—N is the number under consideration,

$n = \lambda N$ is the multiple of N we are attacking,

a is the $\frac{1}{2}$ sum of two complementary factors of n,

b „ $\frac{1}{2}$ difference.

PROP. I.—If every factor of n is congruent to 1 (mod P), where P is any odd integer, then

$$a \equiv 1 \pmod{P}$$

and $$a^2 \equiv n \pmod{P^2}. \qquad \text{(by § 9)}$$

Thus a is limited to 1 case in P^2 (not only to 1 case in P, as stated by misprint in my paper).

PROP. II.—If p be any odd prime, then $a \pmod{p}$ is limited to $\frac{1}{2}(p+1)$ or $\frac{1}{2}(p-1)$ cases, according as n is or is not a quadratic residue of p. (§ 3)

(The table on page 467 of this notice enables these cases to be written out for small values of p.)

PROP. III.—

i. If $n \equiv 5 \pmod 8$, then $a^2 \equiv n+4 \pmod{32}$.
ii. If $n \equiv 1 \pmod 8$, then either $a^2 \equiv n+16 \pmod{128}$
or $a^2 \equiv n \pmod{64}$. (§ 6)

PROP. IV.—If 2 is a quadratic residue of n, so that all factors of n are either $\pm 1 \pmod 8$, then, if $n \equiv 9 \pmod{16}$, we have

$$a^2 \equiv n+16 \pmod{128}. \qquad (\S\ 13)$$

PROP. V.—i. If $n \equiv 2 \pmod 3$, then $a \equiv 0 \pmod 3$. (§ 2)

ii. If $n \equiv 1 \pmod 3$, then $a^2 \equiv n \pmod 9$. (§ 7)

PROP. VI.—

i. If $n \equiv 2 \pmod 5$, then $a \equiv \pm 1 \pmod 5$.
ii. If $n \equiv -2 \pmod 5$, then $a \equiv \pm 2 \pmod 5$.
iii. If $n \equiv \pm 1 \pmod 5$, then either $a \equiv 0 \pmod 5$
or $a^2 \equiv n \pmod{25}$. (§ 8)

PROP. VII.—If no integer from $\sqrt{n}$ up to $\sqrt{n}+t$ is possible as a value of a, there can be no factor of n between

$$\sqrt{n}+t \pm \sqrt{2t\sqrt{n}+t^2}.$$

(This is proved in a paper by me in *Messenger of Mathematics*, Nov., 1894.)

PROP. VIII.—Attacking N directly (*i.e.*, $\lambda = 1$, $n = N$), in order to prove that N has no factor from $\sqrt{N}$ down to $\frac{\sqrt{N}}{k}$, it is only necessary to show that there is no possible value for a from $\sqrt{N}$ up to $\sqrt{N}(1+\Theta)$, where

$$\Theta = \tfrac{1}{2}k\left(1-\frac{1}{k}\right)^2. \qquad (\S\ 16)$$

PROP. IX.—Attacking λN, in order to show that N has no factor from $\sqrt{N}$ down to $\frac{\sqrt{N}}{\lambda}$, it is only necessary to show that there is no possible value for a from $\sqrt{\lambda N}$ up to $\sqrt{\lambda N}+\Theta\sqrt{N}$, where

$$\Theta = \tfrac{1}{2}\lambda\left(1-\frac{1}{\sqrt{\lambda}}\right)^2. \qquad (\S\ 17)$$

The following table enables the possible values of a (mod p), where $p = 5, 7, 11, 13, 17$, or 19, to be written down at once for any value of n:—

Table to find a (mod p).

p	Possible values of a (mod p) satisfying $a^2 - b^2 \equiv 1$ (mod p).	δ	Possible values of a (mod p) satisfying $a^2 - b^2 \equiv \delta$ (mod p).
5	0 or ± 1	2	± 1
7	± 1 or ± 3	-1	0 or ± 1
11	± 1, ± 2, or ± 4	-1	0, ± 2, or ± 5
13	0, ± 1, ± 2, or ± 6	2	± 1, ± 4, or ± 5
17	0, ± 1, ± 3, ± 4, or ± 6	3	± 1, ± 2, ± 4, or ± 6
19	± 1, ± 5, ± 6, ± 8, or ± 9	-1	0, ± 2, ± 4, ± 5, or ± 9

δ is the numerically least non-residue of p.

Now we must be able to write either

$$n \equiv x^2 \,(\text{mod}\, p) \quad \text{or} \quad n \equiv y^2 \delta \,(\text{mod}\, p),$$

according as n is or is not a quadratic residue of p.

And the required values will therefore be found in the first case by multiplying by x those tabulated in the second column, and in the second case by multiplying by y those tabulated in the fourth column.

For, if a_1 satisfies $\quad a_1^2 - b_1^2 \equiv 1 \pmod p$,

then $a_1 x$ satisfies $\quad (a_1 x)^2 - (b_1 x)^2 \equiv x^2 \pmod p$;

and, if a_2 satisfies $\quad a_2^2 - b_2^2 \equiv \delta \pmod p$,

then $a_2 y$ satisfies $\quad (a_2 y)^2 - (b_2 y)^2 \equiv \delta y^2 \pmod p$.

1. $N = 77,843,839,397$.

This number is a residuary factor of $10^{29} - 1$.

Accordingly, it is known that every factor of N is of the form $29m + 1$.* And the tables for residue, index 10, show that N has no factor below 100,000.

* The algebraic factor of $10^{29} - 1$, viz. $(10 - 1)$, and others having been already removed, we also have 10 a quadratic residue; but no advantage can be taken of this here.

Now $$280{,}000 > \surd N > 270{,}000;$$

therefore we need only search for factors from $\surd N$ down to $\frac{\surd N}{2\cdot 8}$. And we can do this by attacking N direct and testing for values of "a" from $\surd N$ up to $\surd N(1+\Theta)$,

where $$\Theta = \frac{2\cdot 8}{2}\left(1-\frac{1}{2\cdot 8}\right)^2 < \cdot 58, \qquad \text{(Prop. VIII.)}$$

so that we need only test for a from 270,000 to 443,000.

Now $N \equiv 1+19\times 29 \pmod{29^2} \equiv 5 \pmod{32} \equiv 2 \pmod 3$;

therefore $a^2 \equiv 1+19\times 29 \pmod{29^2} \equiv 9 \pmod{32}$. (Props. I. and III. i.)

And also $a \equiv 1 \pmod{29}$ and $\equiv 0 \pmod 3$; (Props. I. and V. i.)

therefore $a \equiv 1+24\times 29 \pmod{29^2} \equiv \pm 3 \pmod{16} \equiv 0 \pmod 3$.

Or, combining, $a \equiv 697+20\times 29^2$ or $697+26\times 29^2 \pmod{48\times 29^2}$,

i.e., $a \equiv 17517$ or $22563 \pmod{40368}$.

And we may write $a = 40368x_1+17517$,

or $= 40368x_2+22563$,

where each value of x must be integral, and the limits assigned above to a give $6 < x < 11$.

	mod 5	mod 7	mod 11
Now we have $N \equiv$	2	2	5
therefore we must have $a \equiv$	± 1	± 2 or ± 3	± 3, ± 4, or ± 5
by the table on page 467.			
Moreover $40368 \equiv$	3	6	9
$17517 \equiv$	2	3	5
$22563 \equiv$	3	2	2

Therefore the only values left between the limits	for x_1	and for x_2
after testing for 5 are	8 or 9	7
" " 7 "	8	7
" " 11 "	none	none.

Therefore there is no possible value for a,

and $N = 77{,}843{,}839{,}397$ *is prime.*

2. $N = 182{,}521{,}213{,}001$.

This number is a residuary factor of $10^{25}-1$.

Accordingly, every factor of N is of the form $25m+1$; also 10 is a quadratic residue of every factor; hence here 2 is a quadratic residue, and all factors must be of the form $8m\pm 1$. Moreover, N is known from the tables for residue, index 10, to have no factor $< 100{,}000$.

Now $$430{,}000 > \sqrt{N} > 420{,}000;$$

therefore we need only search for factors of N from $\sqrt{N}$ down to $\frac{\sqrt{N}}{4{\cdot}3}$.

As before, we attack N direct, searching for values of "a" from $\sqrt{N}$ up to $\sqrt{N}(1+\Theta)$, where

$$\Theta = \frac{4{\cdot}3}{2}\left(1-\frac{1}{4{\cdot}3}\right)^2 < 1{\cdot}3; \qquad \text{(Prop. VIII.)}$$

therefore we need only test for "a" from 420,000 up to 990,000.

Now $$N \equiv 1+20\times 25 \pmod{25^2};$$

therefore $$a \equiv 1+10\times 25 \pmod{25^2}. \qquad \text{(Prop. I.)}$$

Moreover $$N \equiv 9 \pmod{16};$$

therefore $$a^2 \equiv N+16 \pmod{128}; \qquad \text{(Prop. IV.)}$$

therefore, since $$N \equiv 73 \pmod{128},$$

$$a^2 \equiv 89 \pmod{128} \quad \text{and} \quad a \equiv \pm 27 \pmod{64}.$$

And $$N \equiv 2 \pmod 3;$$

therefore $$a \equiv 0 \pmod 3. \qquad \text{(Prop. V. i.)}$$

Combining,

$$a \equiv 251+10\times 25^2 \text{ or } 251-32\times 25^2 \pmod{3\times 64\times 25^2},$$

i.e., $$a \equiv 6501, \text{ or } -19749 \pmod{120{,}000}.$$

And we may write $$a = 120{,}000x_1+6501,$$

or $$= 120{,}000x_2-19749,$$

where x_1 and x_2 are integers, and for either we have

$$3 < x < 9$$

(from a consideration of the limits of "a" given above).

	mod 7	mod 11	mod 13	mod 17
Now $N\equiv$	1	6	10	4
therefore we must have $a\equiv$	± 1, or ± 3	0, ± 2 or ± 3	0, ± 1, ± 3 or ± 6	0, ± 2, ± 5, ± 6, ± 8
from tables, p. 467.				
Further $120{,}000\equiv$	-1	1	10	-3
$6501\equiv$	5	0	1	7
$-19749\equiv$	-2	-4	-2	5

Therefore the only possible values left	for x_1	and for x_2
after testing for 7 are	4, 6, or 8	4, 6, or 8
" " 11 "	8	4 or 6
" " 13 "	8	4 or 6
" " 17 "	8	none.

On trial $(8\times 120{,}000+6501)^2-N = 751{,}602{,}970{,}000$,

and this evidently cannot be a perfect square; therefore no value of a satisfies, and

$$N = 182{,}521{,}213{,}001 \textit{ is prime.}$$

3. $N = 1{,}001{,}523{,}179$.

N is a residuary factor of $3^{23}-1$. In fact,

$$3^{23}-1 = 94N.$$

Every possible factor of N is congruent to 1 (mod 23), and also, since 3 is a quadratic residue, is of the form ± 1 (mod 12).

Moreover, since we have to search all the way from $\sqrt{N}$ downwards for factors of N, it will be well to attack a multiple of N.

Selecting $47N\left(i.e., \dfrac{3^{23}-1}{2}\right)$ as our value of "n," we shall be able to search for all factors of N from $\sqrt{N}$ to $\dfrac{\sqrt{N}}{47}$ by searching for values of a from $\sqrt{47N}$ up to $\sqrt{47N}+\Theta\sqrt{N}$, where

$$\Theta = \frac{47}{2}\left(1-\frac{1}{\sqrt{47}}\right)^2 < 17{\cdot}2; \qquad \text{(Prop. IX.)}$$

therefore we have to search for a from 210,000 up to 770,000:

Moreover, since $47 \equiv 1 \pmod{23} \equiv -1 \pmod{12}$, all factors of n are of the forms $23m+1$, $12m' \pm 1$.

And a pair of complementary factors of n [which $\equiv 13 \pmod{24}$] must evidently either be $24m''+1$ and $24m'''+13$, or else $24m''-1$ and $24m'''-13$.

So that we have $\qquad a = \pm 5 \pmod{12}. \qquad (\alpha)$

Now

$$\left.\begin{array}{l} n \equiv 1+14\times 23 \pmod{23^2} \equiv \;\; 5 \pmod{32} \equiv \;\; 4 \pmod 9; \\ \text{therefore} \\ a^2 \equiv 1+14\times 23 \pmod{23^2} \equiv \;\; 9 \pmod{32} \equiv \;\; 4 \pmod 9; \\ \text{therefore} \\ a \equiv 1+\;\, 7\times 23 \pmod{23^2} \equiv \pm 3 \pmod{16} \equiv \pm 2 \pmod 9. \end{array}\right\}$$

(Props. I., III., V.)

Combining the last two results, we obtain

$$a \equiv 29,\ 61,\ 83, \text{ or } 115 \pmod{144}.$$

But, since, by (α), $\qquad a \equiv \pm 5 \pmod{12}$,

61 and 83 are rendered impossible. Thus, finally,

$$a \equiv 1+7\times 23+23^2 \quad\text{or}\quad 1+7\times 23+107\times 23^2 \pmod{144\times 23^2},$$

i.e., $a \equiv 691$ or $56765 \pmod{76176}$.

And we may write

$$a = 76176x_1+691 \quad\text{or}\quad = 76176x_2+56765,$$

where, owing to the limits for a, $2 < x_1 < 11$, $2 < x_2 < 10$.

		mod 5	mod 7	mod 11	mod 13	mod 17
Now	$n \equiv$	3	2	2	4	5
therefore by tables, p. 467, we must have	$a \equiv$	± 2	± 2, or ± 3	0, ± 4 or ± 5	0, ± 1, ± 2 or ± 4	± 1, ± 2, ± 3 or ± 8
Further	$76176 \equiv$	1	2	1	9	-1
	$691 \equiv$	1	5	9	2	11
	$56765 \equiv$	0	2	5	7	2

		for x_1	for x_2
therefore the only possible values left	after testing for 5 are	6 or 7	3, 7, or 8
"	" 7 "	6 or 7	7 or 8
"	" 11 "	6 or 7	none
"	" 13 "	6 or 7	
"	" 17 "	none.	

Thus there are no factors of N lying between $\sqrt{N}$ and $\frac{\sqrt{N}}{47}$, and it only remains for us to try factors below $\frac{\sqrt{N}}{47}$, *i.e.*, below 700. Only three primes below 700 satisfy the required conditions; these are 47, 277, 599. And none of these divide N.

Therefore $N = 1{,}001{,}523{,}179$ *is prime.*

4. $N = 12{,}014{,}633$. (See bottom of p. 474.)

Here it is known that any factor must be of the form $7m+1$.

Now $N \equiv 1 \pmod 8 \equiv 2 \pmod 3$.

Therefore, in order to obtain n of the form 5 (mod 8) and 1 (mod 3), we attack $29N$, and, in order to search for factors from $\sqrt{N}$ down to $\frac{\sqrt{N}}{29}$, we search for values of a from $\sqrt{29N}$ up to

$$\sqrt{29N} + \frac{29}{2}\left(1 - \frac{1}{\sqrt{29}}\right)^2 \sqrt{N}.$$

This will be done if we search from 18,500 up to 54,000.

$$\left.\begin{aligned} \text{Now } 29N &\equiv 5 \pmod{32} \equiv 4 \pmod 9 \equiv 1+7 \pmod{49}; \\ \text{therefore } a^2 &\equiv 9 \pmod{32} \equiv 4 \pmod 9 \equiv 1+7 \pmod{49}; \\ \text{therefore } a &\equiv \pm 3 \pmod{16} \equiv \pm 2 \pmod 9 \equiv 1+4\times 7 \pmod{49}. \end{aligned}\right\}$$

(Props. I., III., V.)

Combining, $a \equiv 29, 61, 83$, or $115 \pmod{144}$, and $\equiv 29 \pmod{49}$;

therefore $a \equiv 29,\ 29+54\times 49,\ 29+80\times 49$, or $29+134\times 49$

$$(\text{mod } 49\times 144),$$

i.e., $a \equiv 29,\ 2675,\ 3949$, or $6595 \pmod{7056}$.

And we may put

$$a = 7056x_1 + 29 \quad \text{or} \quad 7056x_2 + 2675,$$

or

$$7056x_3 + 3949 \quad \text{or} \quad 7056x_4 + 6595.$$

And, from the limits of a, $2 < x < 8$ for x_1, x_2, x_3,

$$1 < x < 7 \quad \text{,,} \quad x_4.$$

		mod 5	mod 11	mod 13
Now	$29N \equiv$	2	6	6
therefore we must have	$a \equiv$	± 1	$0, \pm 2$, or ± 3	$\pm 3, \pm 4$, or ± 6
Also	$7056 \equiv$	1	5	10
	$29 \equiv$	4	7	3
	$2675 \equiv$	0	2	10
	$3949 \equiv$	4	0	10
	$6595 \equiv$	0	6	4

Thus there are left possible values of	x_1	x_2	x_3	x_4
after testing for 5	5, 7	4, 6	5, 7	4, 6
,, ,, 11	7	4	5, 7	6
,, ,, 13	none	none	none	none.

Thus there is no factor between $\sqrt{N}$ and $\frac{\sqrt{N}}{29}$, and the only primes below this limit satisfying the required conditions are 29, 43, 71, 113.

And none of these divide N; therefore

$$N = 12{,}014{,}633 \textit{ is prime.}$$

5. $N = 13{,}477{,}969$. (See bottom of p. 474.)

All factors are of the form $7m+1$.

We have $\qquad N \equiv 1 \pmod 8 \equiv 1 \pmod 3$,

and we might multiply by 29 or 43, and proceed somewhat as before, or proceed directly with N as shown below.

Thus $N \equiv 1 + 80 \pmod{128} \equiv 1 \pmod 9 \equiv 1 + 4 \times 7 \pmod{7^2}$.

And either $\qquad a^2 \equiv 81 + 16 \pmod{128}$ or $\equiv 81 \pmod{64}$;

(Prop. III.)

also $a^2 \equiv 1 \pmod 9 \equiv 1+4\times 7 \pmod{7^2}$.

Thus either $a \equiv \pm 49 \pmod{64}$ or $\equiv \pm 9 \pmod{32}$,

and $a \equiv \pm 1 \pmod 9 \equiv 1 \pm 2\times 7 \pmod{7^2}$.

Combining, either

$$a \equiv 64 \pm 49 \pmod{64\times 49} \quad \text{or} \quad a \equiv 407 \text{ or } 1289 \pmod{32\times 49},$$

and $a \equiv \pm 1 \pmod 9$.

Finally, either

$$a \equiv 3151,\ 9521,\ 15695, \text{ or } 25201 \pmod{28224},$$

or $a \equiv 5111,\ 5993,\ 6679, \text{ or } 7561 \pmod{14112}$.

And, in order to search for factors from $\sqrt{N}$ down to $\frac{\sqrt{N}}{16}$, we must have "a" running from $\sqrt{N}$ up to $\sqrt{N}\left[1+\frac{16}{2}\left(1-\frac{1}{16}\right)^2\right]$, (Prop. VIII.) and to do this we search from 3,600 up to 30,000.

Now $N \equiv 19 \pmod{25}$;

therefore either $a \equiv 0 \pmod 5$ or $a^2 \equiv 19 \pmod{25}$, (Prop. VI.)

i.e., " $a \equiv 0 \pmod 5$ or $a \equiv \pm 12 \pmod{25}$,

and the only values between the limits which are possible are

15695 or 20105 (*i.e.*, 5993+14112).

Now, mod 11:—$N \equiv 10$; therefore a must be 0, ± 2, or ± 5;

$15695 \equiv -2$ and satisfies;

$20105 \equiv -3$ and fails.

And mod 13:—$N \equiv -2$; therefore a must be ± 1, ± 5, or ± 6;

$15695 \equiv 4$ and fails.

Therefore there is no factor of N between $\sqrt{N}$ and $\frac{\sqrt{N}}{16}$.

Below this limit the only possible primes are 29, 43, 71, 113, 127, 197, 211.

None of these divide N. Therefore

$N = 13{,}477{,}969$ *is prime.*

[*Note.*—12,014,633 and 13,477,969 are norms of 7ic trinomial integers

$$N = X^2+7Y^2 = N_7 \quad (a+2b\rho+b\rho^5),$$

$N_7 f(\rho)$ denoting $\quad f(\rho) \,.\, f(\rho^2) \dots f(\rho^6)$,

ρ a true 7th root of 1.

Thus $\quad N_7(1+16\rho+8\rho^5) = 3221^2+7\,.\,484^2 = 12{,}014{,}633$,

$\qquad\quad N_7(3+16\rho+8\rho^5) = 3471^2+7\,.\,452^2 = 13{,}477{,}969$.

They were sent by Col. Cunningham to Mr. Bickmore, who sent them to me.]

An Extension of the Theorem $\dfrac{\Pi(\gamma-a-\beta-1)\,\Pi(\gamma-1)}{\Pi(\gamma-a-1)\,\Pi(\gamma-\beta-1)} = F_1(a, \beta, \gamma)$.

By the Rev. F. H. Jackson, M.A. Received March 27th, 1897. Read April 8th, 1897.

1.

The chief object of this paper is to investigate the following theorem :—

$$\underset{\kappa=\infty}{\mathrm{L}} \frac{(p^{\gamma-\beta}-1)\dots(p^{\gamma-\beta+\kappa-1}-1)}{(p^{\gamma-\beta-a}-1)\dots(p^{\gamma-\beta-a+\kappa-1}-1)}\,\frac{(p^{\gamma-a}-1)\dots(p^{\gamma-a+\kappa-1}-1)}{(p^{\gamma}-1)\dots(p^{\gamma+\kappa-1}-1)}\,p^{a\beta}$$

$$= 1+p^{\gamma-a-\beta}\,\frac{(p^a-1)(p^\beta-1)}{(p^\gamma-1)(p-1)}$$

$$+p^{2(\gamma-a-\beta)}\,\frac{(p^a-1)(p^{a+1}-1)(p^\beta-1)(p^{\beta+1}-1)}{(p^\gamma-1)(p^{\gamma+1}-1)(p-1)(p^2-1)}+\dots,$$

which may be written

$$\frac{\Pi(p^{\gamma-a-\beta-1})\,\Pi(p^{\gamma-1})}{\Pi(p^{\gamma-a-1})\,\Pi(p^{\gamma-\beta-1})} = F_1(p^a.p^\beta.p^\gamma). \tag{A}$$

When $p=1$, the series (A) reduces to the hypergeometric series in which the element x equals unity. The series is convergent for all values of $p>1$, and, if $p=1$, subject to the condition $\gamma-a-\beta>0$.

2.

Let $\left\{\begin{matrix} a \\ n \end{matrix}\right\}$ denote the function

$$\underset{\kappa=\infty}{\mathrm{L}} \frac{(p^{a-n+1}-1)(p^{a-n+2}-1)\dots(p^{a-n+\kappa}-1)}{(p^{a+1}-1)(p^{a+2}-1)\dots(p^{a+\kappa}-1)}$$

$$\times\,\frac{(p^{n+1}-1)(p^{n+2}-1)\dots(p^{n+\kappa}-1)}{(p-1)(p^2-1)\dots(p^\kappa-1)}\,p^{\kappa(a-n)}. \tag{1}$$