proportional to the corresponding trilinear coordinate of Ω_2.

Similar results may be obtained for Ω_1, the first Brocard point.

References

1. N. Altshiller-Court, College Geometry, 2nd ed., 1952, pp. 274–284.
2. R. A. Johnson, Modern Geometry, Boston, 1929, pp. 263–289.
3. C. Smith, Conic Sections, London, 1924, pp. 341–365.

FIBONACCI SERIES MODULO m

D. D. WALL, IBM Corporation

This inquiry is concerned with determining the length of the period of the recurring series obtained by reducing a Fibonacci series by a modulus m. The problem arose in connection with a method for generating random numbers, but it turned out to be unexpectedly intricate, and so quickly became of interest in its own right. The function studied (length of period as a function of starting values and modulus) exhibits quite a few apparent properties which are established here. At least two questions remain unanswered: see remarks after Theorems 5 and 7.

Let f_n denote the nth member of the Fibonacci series $f_0=a$, $f_1=b$, $f_{n+1}=f_n+f_{n-1}$. We reduce f_n modulo m, taking least nonnegative residues, and let h denote the length of the period of the repeating series that results. The letter p is reserved to designate a prime, but a, b, and m may be arbitrary integers, except that we assume, without loss of generality, that a, b, and m are relatively prime: $(a, b, m)=1$. We will also refer to the two special Fibonacci series u_n and v_n defined by $u_0=0$, $u_1=1$, and $v_0=2$, $v_1=1$, and will make use of many of the known properties of these series. It will be convenient to let $k=k(m)$ denote the length of the period of $u_n \pmod m$, in distinction from h which depends on a and b as well as m.

Example: The values of $u_n \pmod 7$ are 0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, and then repeat; so $k(7)=16$. We are curious as to the relation between the number 16 and the number 7. Note that $u_8\equiv 0 \pmod 7$ so the 16 terms in the period form two sets of 8 terms each, the terms of the second half being 6, or -1, times the corresponding terms of the first half. Theorem 7 generalizes this property and explains the relation $k(7)=16$.

THEOREM 1. *$f_n \pmod m$ forms a simply periodic series. That is, the series is periodic and repeats by returning to its starting values.*

Proof. The series repeats because there are only a finite number m^2 of pairs of terms possible, and the recurrence of a pair results in recurrence of all following terms. From the defining relation we have $f_{n-1}=f_{n+1}-f_n$, so if $f_{t+1}\equiv f_{s+1}$ and $f_t\equiv f_s$, (mod m), then $f_{t-1}\equiv f_{s-1}, \cdots, f_{t-s+1}\equiv f_1$, and $f_{t-s}\equiv f_0$, so that the series is simply periodic.

COROLLARY. $u_k\equiv 0$ (mod m). (A direct consequence of Theorem 1.)

THEOREM 2. *If m has the prime factorization $m=\prod p_i^{e_i}$ and if h_i denotes the length of the period of f_n (mod $p_i^{e_i}$), then $h=\text{lcm }[h_i]$, the least common multiple of the h_i.*

Proof. The statement, "h_i is the length of the period of f_n (mod $p_i^{e_i}$)," implies that the series f_n (mod $p_i^{e_i}$) repeats only after blocks of length ch_i; and the statement, "h is the length of the period of f_n (mod m)," implies that f_n (mod $p_i^{e_i}$) repeats after h terms for all values of i. Therefore h is of the form ch_i for all values of i, and since any such number gives a period of f_n (mod m), we conclude that $h=\text{lcm }[h_i]$.

In view of Theorem 2, we may henceforth assume that m is of the form $m=p^e$.

The next five theorems establish properties of the special series u_n with $u_0=0$, $u_1=1$; k is the length of the period of this series, mod m. A close relationship between the special series u_n and the more general series f_n is contained in the formula $f_n=bu_n+au_{n-1}$, which shows that f_n repeats after k terms, so that h is a divisor of k: $h\mid k$.

THEOREM 3. *The terms for which $u_n\equiv 0$ (mod m) have subscripts that form a simple arithmetic progression. That is, $n=xd$ for $x=0, 1, 2, \cdots$, and some positive integer $d=d(m)$, gives all n with $u_n\equiv 0$ (mod m).*

Proof. From the known relations $(u_n, u_{n+1})=1$ and $u_{n+t}=u_{n+1}u_t+u_nu_{t-1}$, we see that $u_i\equiv 0$ (mod m) and $u_j\equiv 0$ (mod m) imply $u_{i+j}\equiv 0$ (mod m) and (with $i\geqq j$) $u_{i-j}\equiv 0$ (mod m). The first follows by setting $n=i$, $t=j$; and setting $n+t=i$, $n=j$ gives $u_{n+1}u_t\equiv 0$ (mod m), which with $(u_n, u_{n+1})=1$ along with $u_n\equiv 0$ (mod m) gives the second congruence $u_t=u_{i-j}\equiv 0$ (mod m). Therefore, the subscripts n that we are concerned with comprise the nonnegative terms of a module, and so are of the form $n=xd$. The corollary to Theorem 1 shows that u_0 is not the only $u_n\equiv 0$ (mod m), so $d>0$, and this completes the proof of the theorem.

Remark. We note that $d\mid k$. Empirically we find many m with $d=k$, but also many with $d<k$.

THEOREM 4. *If $m>2$ then k is an even number.*

Proof. Suppose that k is odd: $k=2x+1$. Then by working both ends to the middle with the defining relation, all congruences being mod m, we find:

$$-u_k \equiv 0 = u_0, \quad u_{k-1} \equiv 1 = u_1, \quad -u_{k-2} = -u_k + u_{k-1} \equiv u_0 + u_1 \equiv u_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(-1)^{t-1}u_{k-t} = (-1)^{t-1}u_{k-t+2} + (-1)^t u_{k-t+1} \equiv u_{t-2} + u_{t-1} = u_t,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(-1)^{x-2}u_{x+2} \equiv u_{x-1}, \qquad (-1)^{x-1}u_{x+1} \equiv u_x.$$

From this last congruence and the defining relation, it follows that $u_{x-1} \equiv 0 \pmod{m}$ if x is odd, and $u_{x+2} \equiv 0 \pmod{m}$ if x is even; but then the congruence just prior to the last one in the sequence shows that again $u_{x-1} \equiv 0 \pmod{m}$.

Now from Theorem 3, $d \mid (x-1)$ so $d \mid (2x-2)$, also $d \mid k$ so $d \mid (2x+1)$; therefore, $d \mid (2x+1-2x+2)$ so $d=3$. Finally $u_d = u_3 = 2 \equiv 0 \pmod{m}$ shows $m=2$ is implied by the hypothesis that k is odd. Therefore for $m>2$, k must be even.

THEOREM 5. *If $k(p^2) \neq k(p)$, then $k(p^e) = p^{e-1}k(p)$. Also, if t is the largest integer with $k(p^t) = k(p)$, then $k(p^e) = p^{e-t}k(p)$ for $e>t$.*

Proof. By solving the standard formulas $u_n = (r^n - s^n)/\sqrt{5}$ and $v_n = r^n + s^n$ for r^n and s^n in terms of u_n and v_n (where r and s satisfy $x^2 = x+1$), expanding $(r^n)^a$ and $(s^n)^a$ by the binomial theorem, and recombining, we obtain the relations

$$\begin{aligned} u_{an} &= (r^{an} - s^{an})/\sqrt{5} = [2^{-a}(\sqrt{5}u_n + v_n)^a - 2^{-a}(-\sqrt{5}u_n + v_n)^a]/\sqrt{5} \\ &= 2^{1-a} \sum_{j \text{ odd}} \binom{a}{j} 5^{(j-1)/2} u_n^j v_n^{a-j} = 2^{1-a} u_n (K u_n^2 + a v_n^{a-1}), \end{aligned}$$

where K is an integer, and similarly

$$\begin{aligned} u_{an+1} &= 5^{-1/2} 2^{-a} \sum_0^a \binom{a}{j} 5^{j/2} u_n^j v_n^{a-j} \left[\frac{1+\sqrt{5}}{2} - (-1)^j \frac{1-\sqrt{5}}{2} \right] \\ &= 2^{-a}(K u_n^2 + a u_n v_n^{a-1} + v_n^a), \end{aligned}$$

where K is an integer. The theorem follows from these relations by induction on e, except for the case $p=2$. We will outline the induction step, observing that the theorem is trivially true for $e=1$ ($e=t$ in the second statement), which enables the induction to begin.

On noting that $v_n = u_{n-1} + u_{n+1}$ has a g.c.d. with u_n of either 1 or 2, and applying Theorem 3, the first formula above gives the "law of repetition of primes": *if u_n is the first term* $\equiv 0 \pmod{p^e}$ *but* $\not\equiv 0 \pmod{p^{e+1}}$, *then u_{pn} is the first term* $\equiv 0 \pmod{p^{e+1}}$, *also* $u_{pn} \not\equiv 0 \pmod{p^{e+2}}$. For this value of n, the terms u_{nx} for $x = 0, 1, 2, \cdots$ are the terms $\equiv 0 \pmod{p^e}$, and u_{pnx} gives all terms $\equiv 0 \pmod{p^{e+1}}$. On setting $u_{pnx+1} \equiv 1 \pmod{p^{e+1}}$, to obtain $k(p^{e+1}) = pnx$, the second formula above gives

$$(v_{nx}/2)^p \equiv 1 \pmod{p^{e+1}},$$
$$v_{nx} \equiv 2 \pmod{p^e}, \qquad u_{nx+1} \equiv 1 \pmod{p^e},$$

so $k(p^e)=nx$ and $k(p^{e+1})=pk(p^e)$. For the exceptional case $p=2$ we use the formulas $u_{2n}=u_n(u_{n-1}+u_{n+1})$ and $u_{2n+1}=u_{n+1}^2+u_n^2$ to establish by induction that $k(2^e)=2^{e-1}k(2)$; the details are omitted here.

Remark. The most perplexing problem we have met in this study concerns the hypothesis $k(p^2)\neq k(p)$. We have run a test on a digital computer which shows that $k(p^2)\neq k(p)$ for all p up to 10,000; however, we cannot yet prove that $k(p^2)=k(p)$ is impossible. The question is closely related to another one, "can a number x have the same order mod p and mod p^2?", for which rare cases give an affirmative answer (*e.g.*, $x=3$, $p=11$; $x=2$, $p=1093$); hence, one might conjecture that equality may hold for some exceptional p.

THEOREM 6. *If* $m=p=10x\pm 1$, *then* $k(p)\mid(p-1)$.

LEMMA. *The congruence* $x^2\equiv x+1 \pmod p$ *has a double root only for* $p=5$.

Proof of Lemma. $x^2-x-1\equiv(x-r)^2$ implies $2r\equiv 1$ and $r^2\equiv -1$; these give $4r^2\equiv 1$ and $4r^2\equiv -4$, so $5\equiv 0$ which implies a modulus of 5.

Proof of Theorem 6. The number 5 is a quadratic residue for primes of the form $p=10x\pm 1$, so the congruence $x^2\equiv x+1 \pmod p$, which is equivalent to $(2x-1)^2\equiv 5 \pmod p$, has distinct roots r and s; therefore $u_n\equiv(r^n-s^n)/(r-s) \pmod p$.

Let g denote the lcm of the order of $r \pmod p$ and the order of $s \pmod p$. Since $rs\equiv -1 \pmod p$, we see that g is equal to the order of r if this number is even, and otherwise is equal to twice the order of r. In either case, $u_n \pmod p$ repeats after g terms, so $k(p)\mid g$, and Fermat's theorem shows $g\mid(p-1)$, so the theorem is proved.

THEOREM 7. *If* $m=p=10x\pm 3$, *then* $k(p)\mid(2p+2)$.

Proof. The number 5 is a quadratic nonresidue for primes of this form, so $5^{(p-1)/2}\equiv -1 \pmod p$. We let $n=p$ and then let $n=p+1$ in the known formula

$$u_n = 2^{1-n}\left[\binom{n}{1}+5\binom{n}{3}+5^2\binom{n}{5}+\cdots\right].$$

The first substitution gives

$$u_p \equiv 5^{(p-1)/2}\binom{p}{p} \equiv -1 \pmod p,$$

and, the second gives

$$u_{p+1} \equiv 2^{-1}\left[\binom{p+1}{1}-\binom{p+1}{p}\right] \equiv 0 \pmod p.$$

These congruences and the defining relation show that $u_{p+2}\equiv -u_1$, $u_{p+3}\equiv -u_2$, $\cdots$, $u_{2p+1}\equiv -u_p\equiv 1$, $u_{2p+2}\equiv -u_{p+1}\equiv 0 \pmod p$. Therefore, $u_n \pmod p$ repeats beginning with $u_{2p+2}\equiv u_0$, so that $k(p)\mid(2p+2)$.

COROLLARY. *If $p=10x\pm 3$ then $k(p)\equiv 0 \pmod 4$.*

Proof. Otherwise $k(p)$ would divide $(p+1)$ which would imply $u_p\equiv +1$.

Remarks. Theorems 6 and 7 furnish upper bounds for the function $k(p)$, and we easily find cases where $k(p)$ has these maximum values. On the other hand, we cannot find a nontrivial lower bound for $k(p)$, and a table of values of $k(p)$ shows many entries with $k(p)$ smaller than the upper limits of Theorems 6 and 7. Examples: $k(491)=490$, $k(521)=26$, $k(4993)=9988$, $k(9349)=38$.

We now return to the more general series f_n. One of the most interesting properties of h, the length of the period of $f_n \pmod m$, is that it is often independent of the starting values a and b. Theorems 8–12 describe this property. In such cases we will write $h=h(m)$, and relate h to $k(m)$, the length of the period of $u_n \pmod m$.

THEOREM 8. *If $p=10x\pm 3$, then $h(p^e)=k(p^e)$.*

Proof. The congruences which indicate that $f_n \pmod m$ repeats with period h may be written in the following form:

$$f_h - a = bu_h + a(u_{h-1} - 1) \equiv 0 \pmod m,$$
$$f_{h+1} - b = (b + a)u_h + b(u_{h-1} - 1) \equiv 0 \pmod m.$$

Considering a and b as given coefficients, the determinant of this system is $D=b^2-ab-a^2$. With $m=p^e$, if $D\equiv 0 \pmod p$ then $4a^2+4ab+b^2=(2a+b)^2 \equiv 5b^2 \pmod p$; and $b\not\equiv 0 \pmod p$ simultaneously with $D\equiv 0 \pmod p$ since this would imply $a\equiv 0 \pmod p$, contradicting $(a, b, m)=1$. Therefore $D\equiv 0 \pmod p$ implies that 5 is a quadratic residue of p. But 5 is not a quadratic residue of primes $p=10x\pm 3$, so for these p and $m=p^e$ we have $(D, m)=1$ and the only solution to the system of congruences is $u_h\equiv 0$, $u_{h-1}\equiv 1 \pmod{p^e}$, which shows that $k \mid h$. Since also $h \mid k$, we therefore have $h=k$, and the theorem is proved.

COROLLARY. *Whenever $D=b^2-ab-a^2$ satisfies $(D, m)=1$, then $h=k$. In particular, v_n has $D=-5$ so if $(5, m)=1$, then the length of the period of v_n* $\pmod m$ *is $k(m)$.*

THEOREM 9. *If $m=2^e$, then $h=k$, and if $m=5^e$, then either $h=k$ or else $h=(1/5)k$, according as $D=b^2-ab-a^2$ is not or is divisible by* 5.

Proof. As in Theorem 8, we examine the determinant D. By observing the three cases with $(a, b, 2)=1$, we see that $D\not\equiv 0 \pmod 2$, so $(D, 2^e)=1$ and $h=k$ for $m=2^e$. If a and b give $D\not\equiv 0 \pmod 5$, then $h=k$ for $m=5^e$. Although it is possible to have $D\equiv 0 \pmod 5$, the congruence $(2a+b)^2\equiv 5b^2 \pmod m$, which is equivalent to $D\equiv 0 \pmod m$, shows that $D\not\equiv 0 \pmod{5^2}$. In this case the congruences $f_h-a\equiv 0 \pmod{5^e}$ and $f_{h+1}-b\equiv 0 \pmod{5^e}$, from Theorem 8, give $u_h\equiv 0 \pmod{5^{e-1}}$ and $u_{h+1}\equiv 1 \pmod{5^{e-1}}$, so $k(5^{e-1}) \mid h(a, b, 5^e)$ and $h(a, b, 5^e)$ $=$either $k(5^e)$ or $(1/5)k(5^e)$. But the second value always holds, for $D\equiv 0 \pmod 5$ implies $b=-2a+5t$, and the formula

$$u_n = 2^{1-n}\left[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots\right]$$

shows that $u_{(1/5)k(5^e)} = u_{4\cdot 5^{e-1}} \equiv 3\cdot 5^{e-1} \pmod{5^e}$ and $u_{4\cdot 5^{e-1}+1} \equiv 1+4\cdot 5^{e-1} \pmod{5^e}$, since the terms $5\binom{n}{3}$, $5^2\binom{n}{5}$, $\cdots$, are all divisible by 5^e. Therefore $f_{(1/5)k(5^e)} \equiv (-2a+5t)\cdot 3\cdot 5^{e-1} + a(1+5^{e-1}) \equiv a \pmod{5^e}$, and $f_{(1/5)k(5^e)+1} \equiv (-2a+5t)\cdot(1+4\cdot 5^{e-1}) + a(3\cdot 5^{e-1}) \equiv b \pmod{5^e}$. These formulas require $e>1$, but for, $e=1$, an enumeration of cases shows $k=20$ and $h=20$ for $D\not\equiv 0 \pmod 5$ and $h=4$ when $D\equiv 0 \pmod 5$, so the theorem is proved.

COROLLARY. *If $m=p^e$ and h is odd, then $p=10x\pm 1$ or $m=2$.*

(A direct consequence of Theorems 4, 8, and 9.)

THEOREM 10. *If $m=p^e$, $p>2$, and if (a, b) give $h=2t+1$, then $k=4t+2$.*

Proof. The congruences which indicate that $f_n \pmod m$ repeats with period h may also be written as follows:

$$bu_h + a(u_{h-1} - 1) \equiv 0 \pmod m,$$
$$b(u_{h+1} - 1) + au_h \equiv 0 \pmod m.$$

The condition $(a, b, m)=1$ implies that $u_h^2-(u_{h+1}-1)(u_{h-1}-1)\equiv 0 \pmod m$, and the known formula $u_h^2-u_{h+1}u_{h-1}=(-1)^{h-1}$ permits this congruence to be simplified to $u_{h+1}+u_{h-1}=v_h=u_{2h}/u_h\equiv 1+(-1)^h \pmod m$. Therefore, h odd implies $u_{2h}\equiv 0 \pmod m$. Since $f_n \pmod m$ also repeats with period $2h$, the analogous congruences stating this fact lead to the analogous condition $u_{2h+1}+u_{2h-1} \equiv 1+(-1)^{2h}=2 \pmod m$, so $u_{2h}=0 \pmod m$ further implies $2u_{2h+1}\equiv 2$, $u_{2h+1} \equiv 1 \pmod m$, so $k\mid 2h$. Finally, k is even since $m>2$, so h odd requires $k=2h$, and the theorem is proved.

Examples:

$m = 11$, $a = 1$, $b = 4$ gives $h = 5$, while $k(11) = 10$;

$m = 29$, $a = 1$, $b = 24$ gives $h = 7$, while $k(29) = 14$;

$m = 121$, $a = 1$, $b = 37$ gives $h = 55$, while $k(121) = 110$.

THEOREM 11. (Converse to Theorem 10.) *If $m=p^e$, $p>2$, and if $k=4t+2$, then $h=2t+1$ for some (a, b).*

LEMMA. *If $k(p^e)=4t+2$, then $u_{2t+2}\equiv -u_{2t} \pmod{p^e}$.*

Proof of Lemma. This condition follows directly from the chain of congruences developed in Theorem 4, k now being even.

Proof of Theorem 11. Let

$$a = f_0 \equiv -u_{2t+1} - u_0 \pmod{p^e}, \qquad b = f_1 \equiv u_{2t} - u_1.$$

Then $f_n \equiv (-1)^{n-1}u_{2t+1-n} - u_n$, so $f_{2t+1} \equiv f_0$ and $f_{2t+2} \equiv -u_{-1} - u_{2t+2} \equiv -u_1 + u_{2t} = f_1$. Therefore $h \mid (2t+1)$; but then Theorem 10 shows $k = 2h$. This completes the proof except it must be verified that $(a, b, p^e) = 1$, which follows from Theorem 4 since $a \equiv -u_{2t+1} - u_0 \equiv b \equiv u_{2t} - u_1 \equiv 0 \pmod p$ would give $k(p) = 2t+1$, which is impossible. Incidentally, the case $p^e = 4$ is actually an exceptional case, since $k(4) = 6 \equiv 2 \pmod 4$, but no series $f_n \pmod 4$ has $h = 3$.

THEOREM 12. *If $m = p^e$, $p > 2$, $p \neq 5$, and h is even, then $h = k$.*

Proof. We use the condition $v_h \equiv 1 + (-1)^h \pmod m$, from Theorem 10, and the relation $v_n = r^n + s^n$ where r and s are the real roots of the equation $x^2 = x + 1$. Then, since h is even, and since $rs = -1$,

$$r^h + s^h - 2 \equiv 0 \pmod m,$$

$$r^{2h} + s^{2h} + 4 + 2(rs)^h - 4r^h - 4s^h \equiv 0 \pmod{m^2},$$

$$r^{2h} - 2 + s^{2h} \equiv (r^h - s^h)^2 \equiv 0 \pmod{m^2}.$$

Now $r^h - s^h$ is not an integer, but is of the form $x\sqrt{5}$; and since $p \neq 5$ assures $5 \not\equiv 0 \pmod m$, we may divide by $5 = (r-s)^2$ to obtain

$$\left[(r^h - s^h)/(r - s)\right]^2 = u_h^2 \equiv 0 \pmod{m^2}, \qquad u_h \equiv 0 \pmod m.$$

Finally $u_h \equiv 0$ and $v_h \equiv 2$ imply $u_{h-1} \equiv u_{h+1} \equiv 1$, which in turn implies $h = k$.

COROLLARY 1. *If $p \neq 5$ and $k(p) \equiv 0 \pmod 4$, then $h(p^e) = k(p^e)$.* (A direct consequence of Theorems 10 and 12, except for $p = 2$ which is covered by Theorem 9.)

COROLLARY 2. *If $h(a, b, p) = k(p)$ and $k(p^2) \neq k(p)$, then $h(a, b, p^e) = k(p^e)$.*

Proof. $h(a, b, p^e)$ must be a multiple of $h(a, b, p) = k(p)$, and must be a divisor of $k(p^e) = p^{e-1}k(p)$, hence must be of the form $p^{-c}k(p^e)$ for $c \geqq 0$. But Theorems 10 and 12 show that $h = k$ or $h = k/2$, so $h(a, b, p^e) = k(p^e)$. The cases $p = 2$ and $p = 5$ are covered by Theorem 9; for $p = 5$ note that $h = k$ or $h = (1/5)k$ independently of e.

Remark. The converse of Corollary 2 is false. For example, $h(3, 1, 11) < k(11)$, but $h(3, 1, 11^2) = k(11^2)$.

Example. Find h and k for $m = 10^{10}$.

As per Theorem 2, we consider $m_1 = 2^{10}$ and $m_2 = 5^{10}$. To apply Theorem 5, we check that $k(2) = 3 \neq k(2^2)$ and $k(5) = 20 \neq k(5^2)$. Therefore $k_1 = 3.2^9$, $k_2 = 20.5^9$, $k = \mathrm{lcm}\,[k_1, k_2] = 15.10^9$. Finally, Theorem 9 shows that $h = 15.10^9$ or $h = 3 \cdot 10^9$ according as $D = b^2 - ab - a^2$ is not or is divisible by 5.

Remark. We note in passing that the number of ordered pairs $(a, b) \pmod m$ with $(a, b, m) = 1$ is given by the formula $m^2 \prod_{p \mid m} (1 - 1/p^2)$.

Since the results of this study direct interest to the function $k(p)$, we append a table of $k(p)$, listing all cases with $5<p<2000$ for which $k(p)$ is smaller than the maximum value permitted by Theorems 6 and 7.

p	$k(p)$	p	$k(p)$	p	$k(p)$
29	14	743	496	1279	426
47	32	761	380	1289	322
89	44	769	192	1291	430
101	50	797	228	1307	872
107	72	809	202	1361	680
113	76	811	270	1381	460
139	46	829	276	1409	704
151	50	859	78	1427	168
181	90	881	176	1471	490
199	22	911	70	1483	424
211	42	919	102	1511	302
229	114	941	470	1523	1016
233	52	953	212	1549	774
263	176	967	176	1553	1036
281	56	977	652	1579	526
307	88	991	198	1597	68
331	110	1009	126	1601	160
347	232	1021	510	1621	810
349	174	1031	206	1669	834
353	236	1049	262	1699	566
401	200	1061	530	1709	854
421	84	1069	356	1721	430
461	46	1087	128	1733	1156
509	254	1097	732	1741	870
521	26	1103	96	1789	894
541	90	1109	554	1823	1216
557	124	1151	230	1861	930
563	376	1217	812	1871	374
619	206	1223	816	1877	1252
661	220	1229	614	1913	1276
677	452	1231	410	1951	390
691	138	1249	624	1973	1316
709	118	1277	852	1999	666

The author wishes to acknowledge the assistance of George E. Collins, who carefully reviewed the paper and made many helpful suggestions.

Reference

L. E. Dickson, History of the Theory of Numbers, vol. 1. Washington, D. C., 1920.