FACTORS OF THE BINOMIAL CIRCULANT DETERMINANT

J. S. FRAME
Michigan State University, East Lansing, MI 48823

1. INTRODUCTION

Interesting problems and patterns in algebra, number theory, and numerical computation have arisen in the attempt to prove or disprove a conjecture known as Fermat's Last Theorem [7], namely that for odd primes p there are no rational integral solutions x, y, z, with $xyz \neq 0$ to the equation

$$x^p + y^p + z^p = 0. \tag{1.1}$$

Several proofs of special cases involve the prime factors of the determinant D_n of the $n \times n$ binomial circulant matrix B_n with (i, j)-entry

$$\binom{n}{|i - j|}.$$

Thus in 1919 Bachmann [1] proved that (1.1) has no solutions prime to p unless $p^3 | D_{p-1}$, and in 1935 Emma Lehmer [6] proved the stronger requirement, $p^{p-1} | D_{p-1}$, mentioning that $D_n = 0$ iff $n = 6k$, and giving the values of D_{p-1} for $3 \leq p \leq 17$. Later, in 1959-60, L. Carlitz published two papers [2, 3] concerning the residues of D_{p-1} modulo powers of p, including the theorem that (1,1) is solvable with $xyz \neq 0$ only if $D_{p-1} \equiv 0 \pmod{p^{p+43}}$. Our methods give, for example when $p = 47$, the prime factorization

$$-D_{46} = 3 \cdot 47^{45}(139^4 461^2 599^4 691^4 829^2 1151^2 2347^2 3313^2 178481 \cdot 2796203)^3 \tag{1.2}$$

Clearly, a nontrivial solution of (1.1) would require that for all primes q not dividing xyz we should have

$$1 + (y/x)^p \equiv (-z/x)^p \pmod{q}. \tag{1.3}$$

For each such prime p and for all primes $q = 1 + np$ not divisors of xyz, we should have

$$(1 + (y/x)^p)^n \equiv 1 \pmod{q}. \tag{1.4}$$

Thus, all primes $q = 1 + np$ except the finite number that divide xyz must divide the corresponding D_n, which is the resolvent of $v^n - 1$ and $(v + 1)^n - v^n$.

Our concern in this paper is to characterize and compute the rational prime factors of the determinant D_n, an integer of about $0.1403n^2$ digits, when $n \not\equiv 0 \pmod 6$. The 351-digit integer $-D_{50}$ was found to have 127 prime factors, counting multiplicities as high as 24 for the factor 101.

To factor D_n we first note that its $n \times n$ binomial circulant matrix B_n is a polynomial in the $n \times n$ circulant matrix P_n for the permutation (1 2 3 ... n), whose eigenvalues are powers of a primitive nth root of unity, r, and that D_n is the product of the eigenvalues of B_n. Thus, as in [5],

$$B_n = (I_n + P_n)^n - I_n \tag{1.5}$$

$$D_n = \prod_{k=1}^{n} ((1 + r^k)^n - 1), \quad \text{where } r = e^{2\pi i/n}. \tag{1.6}$$

For example, when $n = 4$,

$$(1.7)\qquad P_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad B_4 = \begin{bmatrix} 1 & 4 & 6 & 4 \\ 4 & 1 & 4 & 6 \\ 6 & 4 & 1 & 4 \\ 4 & 6 & 4 & 1 \end{bmatrix} = (I_4 + P_4)^4 - I_4$$

$$(1.8)\qquad D_4 = ((1+i)^4 - 1)(0^4 - 1)((1-i)^4 - 1)(2^4 - 1) = -3 \cdot 5^3.$$

Factoring the difference of two nth powers in (1.6) yields

$$(1.9)\qquad D_n = \prod_{k=1}^{n} \prod_{j=1}^{n} ((1 + r^k)r^j - 1) = (-1)^n \prod_{j=1}^{n} \prod_{k=1}^{n} (1 - r^j - r^k).$$

Theorem 1.1 (E. Lehmer [6]): $D_n = 0$ if and only if $6|n$.

Proof: A factor $(1 - r^j - r^k)$ in (1.9) can vanish if and only if $r^k = r^{-j}$, and $r^{6j} = 1$.

Henceforth we assume $n \not\equiv 0 \pmod 6$.

Experimental evidence indicates that for $n \le 50$,

$$(1.10)\qquad \left|\log_{10}|D_n| - n^2 \log_{10} G\right| < 0.33, \text{ if } n \not\equiv 0 \pmod 6,$$

where G is the limit as $n \to \infty$ of the geometric mean of the n^2 factors $|1 - r^j - r^k|$ of $(-1)^{n-1}D_n$. If $u - v = \theta$, we have

$$(1.11)\qquad \ln G = \pi^{-2} \int_0^{\pi} \int_0^{\pi} \ln|1 - e^{2iu} - e^{2iv}|\,du\,dv$$

$$= \pi^{-2} \int_0^{\pi} \int_0^{\pi} \ln|2\cos\theta - e^{-2i\phi}|\,d\phi\,d\theta.$$

The inner integral vanishes if $|2\cos\theta| < 1$, and we obtain

$$(1.12)\qquad \ln G = (2/\pi) \int_0^{\pi/3} \ln(2\cos\theta)\,d\theta = (2/\pi) \int_0^{\pi/6} \theta \cot\theta\,d\theta$$

$$(1.13)\qquad \log_{10} G = (0.32306594722\ldots)/\ln(10) = 0.14030575817\ldots\,.$$

Missing factors in the tables were detected by (1.10), and found.

Our challenge is to assemble the n^2 complex factors of (1.9) into subsets having rational integral products which we call "principal" factors, and then factor these positive integers into their rational prime factors. We find that $(-1)^{n-1}D_n/(2^n - 1)$ is always a square, that $-D_{2n}/3$ is a cube, and that for odd n the sum $F_{n-1} + F_{n+1}$ of two Fibonacci numbers is a double factor of D_n, of about $1 + n/5$ digits, which is frequently prime. For example, D_{47} and D_{53} have respectively as double factors the primes $F_{46} + F_{48} = 6{,}643{,}838{,}879$ and $F_{52} + F_{54} = 119{,}218{,}851{,}371$. Tables 1 and 2 list the prime factors of D_n other than $2^n - 1$ for 16 odd values of n.

TABLE 1

FACTORS $q_p^{(\pm u)}$ OF d_p, WHERE p IS PRIME,
AND UNDERLINED FACTORS ARE $q_p^{(-u)}$

u	d_{19}	d_{23}	d_{29}	d_{31}	d_{37}	d_{41}	d_{43}	d_{47}
2	9349	139 • 461	59 • 19489	3010349	54018521	370248521	969323029	6643838879
3	1483	47 • 139	65657	5^3•1117	1385429	83 • 77081	431•31907	941 • 67399
4	229	1151	9803	27901	132313	83^3	952967	283 • 11939
5	$\underline{761}$	599	59^2	5953	149 • 223	101107	173 • 1033	549149
6	647	$\underline{3313}$	$\underline{24071}$	20089	67489	83^3	516689	1693 • 2351
7	229	47^2	18503	$\underline{16741}$	149•1259	$\underline{83 \cdot 3691}$	173 • 6967	6450751
8	419	47^2	59 • 233	$\underline{46439}$	325379	988511	1124107	$\underline{1352191}$
9	191	2347	4931	38069	223•1481	821 • 1559	745621	7145599
10		$\underline{599}$	$\underline{18097}$	34721	172717	1335781	173 • 2337	283 • 36943
11		691	59 • 349	5953	146891	83 • 6397	$\underline{2532701}$	1223 • 2663
12			12413	2^5•1489	262553	791629	1549•1721	$\underline{10032151}$
13			$\underline{59^2}$	$\underline{2^5 \cdot 683}$	149 • 223	348911	$\underline{1144919}$	2069 • 5077
14			59^2	2^5 • 311	$\underline{332039}$	$\underline{83 \cdot 12301}$	1999243	3462961
15				6263	$\underline{149 \cdot 1999}$	$\underline{206477}$	173 • 1033	1932923
16					$\underline{68821}$	1024099	431 • 5591	$\underline{941 \cdot 8179}$
17					223 • 593	739 • 1723	173•10837	4220977
18					32783	$\underline{340793}$	$\underline{173 \cdot 11783}$	5187109
19						$\underline{101107}$	431 • 3613	$\underline{1129 \cdot 6863}$
20						83 • 1231	533459	1754323
21							178021	$\underline{659 \cdot 3761}$
22								$\underline{549149}$
23								549431

TABLE 2

FACTORS $\overline{q}_n^{(u)}$ OF $\overline{d}_n$ FOR COMPOSITE ODD n

u	$\overline{d}_9$	$\overline{d}_{15}$	$\overline{d}_{21}$	$\overline{d}_{25}$	$\overline{d}_{27}$	$\overline{d}_{33}$	$\overline{d}_{35}$	$\overline{d}_{39}$
3:p		271	2269			176419		$157 \cdot 10141$
5:p							38851	
2	19	31	211	$101 \cdot 151$	5779	9901	$71 \cdot 911$	$79 \cdot 859$
3	37	31	379	1301	811	67^2	7351	22777
−3	19	2^4	43		487	2971		6553
4	1	$2^2 \cdot 1$*	7	3851	919	67	3361	547
5		61	43	1151	109	463	2381	$79 \cdot 3^3$
−5		31		6101			3011	
6		1	463	151	433	331	41*	79^2
−6		61	1		163	3631	29*	1249
7		1	43	251		199	7841	157
−7			547		163		71^2	
8			$1 \cdot 7$*	401	2269	859	71	$79 \cdot 3^3$
9			43	1151	19441	2311		1171
−9			43		19927	397	701	3511
10			7^2	5801	1	43*	$71 \cdot 281$	
−10				1951		1*	71^2	1249
11				101	757	$67 \cdot 661$	71	3121
−11						25411		
12				101	109	1		$79 \cdot 937$
−12					109	$67 \cdot 199$	421	1
13					271	67	5741	$79 \cdot 2887$
−13								398581
14						331	118301	1*
−14							4271	103*
15						397	911	1171
−15						463	211^2	13183
16						67	2381	157
17							211	1483
18								$313 \cdot 3^3$
−18								$79 \cdot 3^3$
19								157

*If $u^2 \equiv 1 \pmod{n}$, $\left(\overline{q}_n^{(u)}\overline{q}_n^{(-u)}\right)^{1/2}$ replaces $\overline{q}_n^{(u)}$ in $\overline{d}_n$.

2. PRINCIPAL INTEGRAL FACTORS OF D_n

For n odd, we extract from D_n in (1.9) the product $1 - 2^n$ of n factors with $j = k$, the product 1 of the $2(n - 1)$ factors with $j = n \neq k$ or $k = n \neq j$, and the product $q_n^{(-1)}$ of the $n - 1$ real factors with $j + k = n$, and are left with $(n - 1)(n - 3)$ factors whose product d_n^2 is a perfect square because of symmetry in j and k.

Theorem 2.1: For n odd, we have

$$D_n = (2^n - 1)q_n^{(-1)}d_n^2, \tag{2.1}$$

where $q_n^{(-1)} = 4$ if $3|n$, $q_n^{(-1)} = 1$ if $n \equiv \pm 1 \pmod 6$, and d_n is a product of $(n-1)(n-3)/4$ conjugate complex factor pairs, namely

$$d_n = \prod_{0<j<k<n-j} (1 - r^j - r^k)(1 - r^{-j} - r^{-k}),\ r = e^{2\pi i/n}. \tag{2.2}$$

Proof: The product of the $(n-1)$ real factors of (1.9) with $1 \leq j \leq n-1$ is

$$q_n^{(-1)} = \prod_{j=1}^{n-1}(1 - r^j - r^{-j}) = \prod_{j=1}^{n-1}(-r^{-j})(r^j + \omega)(r^j + \overline{\omega})$$

$$= 1 \cdot (1 + \omega^n)(1 + \omega^{-n}) = (\omega^{n/2} + \omega^{-n/2})^2 \tag{2.3}$$

$$= (2 \cos \pi n/3)^2$$

where $\omega = e^{2\pi i/3}$. This is 4 if $3|n$, or 1 if $n \equiv \pm 1 \pmod 6$. Of the remaining complex factors with $j + k \neq n$, those with $j + k > n$ are the complex conjugates of those with $j + k < n$. Just half the factors of d_n^2 yield d_n, so we take $j < k$ in (2.2).

For even dimension $2n$ we replace $-r^j$ and $-r^k$ in (1.9) by s^{j+n} and s^{k+n}, where $s = e^{\pi i/n}$ and $s^n = -1$. The factor with 3 equal summands is $1 + 1 + 1 = 3$, and the $3(2n-1)$ factors with 2 equal summands have the product

$$-((4^n - 1)/3)^3.$$

Since $3 \nmid n$, we can divide each of the $(2n-1)(2n-2)$ remaining factors by the geometric mean of its 3 summands so the new factors have distinct summands with product 1.

Theorem 2.2: For even dimension $2n$, we have

$$D_{2n} = -3((4^n - 1)/3)^3 g_{2n}^6, \tag{2.4}$$

where g_{2n} is the product of $(n-1)(n-2)/3$ conjugate complex factor pairs

$$g_{2n} = \prod_{0<j<k<n-j/2} |s^j + s^k + s^{-j-k}|^2,\ s = e^{\pi i/n}. \tag{2.5}$$

Proof: Extracting from D_{2n} the factors with repeated summands leaves a product of $(2n-1)(2n-2)$ factors with distinct summands

$$-9D_{2n}/(4^n - 1)^3 = \prod_{j,k,i=1}^{2n} (s^j + s^k + s^i),\ s^{j+k+i} = 1, \tag{2.6}$$

$$i, j, k \text{ distinct.}$$

We omit the $3(2n-2)$ factors with product 1 having i, j, or $k = 2n$. Symmetry in i, j, k shows that each remaining factor is repeated six times, so we call the product g_{2n}^6, where in g_{2n} we assume $1 \leq j < k < i < 2n$. Since factors with $j + k + i = 4n$ are the complex conjugates of factors with $j + k + i = 2n$, we replace i by $2n - j - k$ and s^i by s^{-j-k} to obtain (2.5).

Theorem 2.3: For odd $n = 2m + 1$ not divisible by 3, $g_{2n} = d_n h_n$ where h_n is the product of $m(m-2)/3$ factor pairs

(2.7) $$h_n = g_{2n}/d_n = \prod_{0<j<k<(n-j)/2} |r^j + r^k + r^{-j-k}|^2, \quad r = e^{2\pi i/n}.$$

Proof: The $m(m - 2)/3$ factor pairs in (2.5) with j and k both even yield the factor pairs of h_n in (2.7). We next delete the m factor pairs in (2.5) for which j or k equals $n - j - k$, since $s^n = -1$ and these factors have the product 1. In the remaining $m(m - 1)$ factor pairs having two summands with odd exponents, we multiply these two summands by $-s^n = 1$ to create even exponents, divide the factor by the third summand, set $s^2 = r$, and obtain precisely the factors of d_n in (2.2).

Note that (2.4) and (2.7) imply that for $n \equiv \pm 1 \pmod 6$

(2.8) $$-D_{2n}/D_n^3 = 3^{-2}(2^n + 1)^3 h_n^6, \text{ if } n = \pm 1 \pmod 6.$$

Theorem 2.4: For $n = 2m$ not divisible by 6, $g_{2n} = g_n k_n$, where k_n is the product of $m(m - 1)$ factor pairs:

(2.9) $$k_n = g_{2n}/g_n = \prod_{0<j<k<2n-j} |1 + s^j + s^k|^2, \quad j, k \text{ odd}, \quad s = e^{\pi i/n}.$$

Proof: The $(m - 1)(m - 2)/3$ factor pairs in (2.5) having j and k both even yield the factor pairs of g_n for even n. We obtain the remaining $m(m - 1)$ factor pairs for k_n in (2.9) by dividing each of the remaining factors of g_{2n} by its summand with even exponent.

If desired, we can remove the $[m/2]$ factor pairs with product 1 in (2.9) for which $k = n + j$. For example, when $m = 2$, one of the two factor pairs in $k_4 = g_8/g_4$ can be removed, leaving

(2.10) $$k_4 = g_8/g_4 = |1 + s + s^3|^2 = |1 + i\sqrt{2}|^2 = 3, \quad s = e^{\pi i/4}.$$

Since $g_4 = g_2 = d_1 = 1$, we have $D_8 = -3(85)^3 \cdot 3^6 = -3^7 \cdot 5^3 \cdot 17^3$. The reduced integral factors $\overline{d}_n$ of d_n and $\overline{h}_n$ of h_n are products of those complex factors of (2.2) or (2.7) in which j, k, n have no common factor.

The extended principal factors of d_n, h_n, and k_{2n} are products of those complex factors of d_n, h_n, or k_{2n} in which the exponent ratios $k:j$ are constant (mod n). They are rational integers, since they are symmetric functions of roots of unity. In such an extended principal factor $q_n^{(v:u)}$, we assume u, v relatively prime and replace (j,k) by (vj,uj) where $0 < j < n$. For $\overline{d}_n$ and $\overline{h}_n$ we restrict j to a reduced set of residues (mod n) denoted R_n, in which $(j,n) = 1$. We define the extended principal factors $q_n^{(v:u)}$ and the principal factors $\overline{q}_n^{(v:u)}$ by

(2.11) $$q_n^{(v:u)} = \pm \prod_{j=1}^{n-1} (1 - r^{vj} - r^{uj}) > 0, \quad q_n^{(u)} = q_n^{(1:u)} = q_n^{(u:1)}$$

(2.12) $$\overline{q}_n^{(v:u)} = \pm \prod_{j \in R_n} (1 - r^{vj} - r^{uj}) > 0, \quad \overline{q}_n^{(u)} = \overline{q}_n^{(1:u)} = \overline{q}_n^{(u:1)}$$

where $r = e^{2\pi i/n}$. The corresponding integral factors of k_n or h_n with complex factors $(1 + r^{vj} + r^{uj})$ are denoted by $q_{n+}^{(v:u)}$, etc. Factors of $q_{n\pm}^{(v:u)}$ for which $(j,n) = n/f$ divide $q_{f\pm}^{(v:u)}$ for divisors f of n.

For calculations with a calculator that computes cosine functions, the following factors are useful. We set

(2.13) $$\overline{f}_n^{(y;x)} = \pm \prod_{j \in R_n} (c_{yj} + c_{yj}^{-1} - c_{xj}) > 0, \quad (x,y) = 1$$

where $c_k = r^k + r^{-k} = 2\cos 2\pi k/n$, and where R_n' denotes the set of $\varphi(n)/2$ residues $j \in R_n$ with $j < n/2$.

Theorem 2.5: If $2x = (u + v)$, $2y = u - v$, then

$$\bar{f}_n^{(y;x)} = \bar{q}_n^{(v:u)},\ \bar{f}_n^{(v;u)} = \bar{q}_n^{(y;x)},\ n \text{ odd.} \tag{2.14}$$

Proof:

$$\begin{aligned} \bar{q}_n^{(v:u)} &= \prod_{j\in R_n'} |1 - r^{vj} - r^{uj}|^2 = \prod_{j\in R_n'} (3 + c_{2yj} - c_{vj} - c_{uj}) \\ &= \prod_{j\in R_n'} (1 + c_{yj}^2 - c_{yj}c_{xj}) = \pm \prod_{j\in R_n'} (c_{yj} + c_{yj}^{-1} - c_{xj}) \end{aligned} \tag{2.15}$$

since the product of the c_{yj} is ± 1. Solving for u,v in terms of x,y yields the second part of (2.14)

Theorem 2.6: If $n = 2m + 1$ is a prime $p > 3$, then

$$d_p = \prod_{u=2}^{m} q_p^{(\varepsilon u)},\ \varepsilon = \pm 1 \tag{2.16}$$

where $\varepsilon = 1$ if $u < u' \equiv 1/u \pmod p$ or $\varepsilon = -1$ if $u' < u < p/2$.

Proof: The product of the $p - 3$ integers $q_p^{(u)}$ for $2 \le u \le p - 2$ is d_p^2. Since $q^{(u')} = q^{(u)}$ if $uu' \equiv 1 \pmod p$, we multiply together one factor from each of these pairs to obtain d_p.

For example

$$\begin{aligned} d_5 &= q_5^{(2)} = f_5^{(3)} = 11;\ d_7 = q_7^{(2)} q_7^{(3)} = f_7^{(3)} f_7^{(2)} = 29 \cdot 8 \\ d_{11} &= q_{11}^{(2)} q_{11}^{(3)} q_{11}^{(-4)} q_{11}^{(5)} = f_{11}^{(3)} f_{11}^{(2)} f_{11}^{(5)} f_{11}^{(-4)} = 199 \cdot 67 \cdot \underline{23} \cdot 23 \\ d_{13} &= \prod_{u=2}^{6} q_{13}^{(u)} = 521 \cdot 131 \cdot 79 \cdot 27 \cdot 53 \\ d_{17} &= 3571 \cdot 613 \cdot 409 \cdot 137 \cdot \underline{307} \cdot \underline{137} \cdot 103. \end{aligned} \tag{2.17}$$

Theorem 2.7: If p^b is a maximal prime power divisor of $q_n^{(u)}$ for prime $n > u > 0$, then $p^b \equiv 1 \pmod n$.

Proof: If $p \mid q_n^{(u)}$, there is a smallest field $GF(p^e)$ of characteristic p that contains a mark $\bar{r}$ such that $\bar{r}^n \equiv 1 \equiv \bar{r} + \bar{r}^u \pmod p$. Raising to pth powers we see that $\bar{r}^{p^k}$ is a solution for $k = 0, 1, \ldots, e - 1$. Since b factors $1 - \bar{r}^j - \bar{r}^{uj}$ vanish $\pmod p$, e divides b. Since the order of $\bar{r} \not\equiv 1$ is a factor of the prime n, it is n. Hence n divides the order $p^e - 1$ of the multiplicative group of $GF(p^e)$, which divides $p^b - 1$.

We find, for example, that $q_7^{(3)} = 2^3$, $q_{13}^{(4)} = 3^3$, and 2^5 divides $q_{31}^{(u)}$ for $u = 12, -13$, and 14. Factors of $q_p^{(u)}$ for primes 19 to 47 are listed in Table 1 above.

When, for composite n, we have $u^2 \equiv 1 \pmod n$ but $u \not\equiv \pm 1 \pmod n$, the factors $q_n^{(u)}$ and $q_n^{(-u)}$ of $\bar{d}_n^2$ are squares without reciprocal mates, so we must include only their square roots in $\bar{d}_n$. Also, $\bar{d}_n$ may include factors $q^{(v:u)}$ where u and v are relatively prime divisors of n. For example, the

$(n-1)(n-3)/2 = 84$ complex factors of d_{15} include $4 \cdot 2/2 = 4$ from d_5 and $2 \cdot 0/2 = 0$ from d_3, leaving 40 complex conjugate pairs in $\overline{d}_{15}$. The latter include four pairs each from $\overline{q}_{15}^{(u)}$ for $u = 2, 3, 5, 6, 7, 9, 10$, and 12, four from $\overline{q}_{15}^{(3:5)}$, but only two pairs each from $\overline{q}_{15}^{(4)} = 16$ and $\overline{q}_{15}^{(-4)} = 1$.

$$\overline{d}_{15} = 31 \cdot 31 \cdot 61 \cdot 1 \cdot 1 \cdot 61 \cdot 31 \cdot 2^4 \cdot 271 \cdot (2^4 \cdot 1)^{1/2}. \tag{2.18}$$

The factor $q_{15}^{(4)}$ was found by (2.13) to be

$$q_{15}^{(4)} = f_{15}^{(3;5)} = (\sqrt{5}+1)^2(-\sqrt{5}+1)^2 = 2^4. \tag{2.19}$$

To evaluate the principal factor $\overline{q}_{3p}^{(3;p)}$ for primes $p \geq 5$, we set

$$r^p = \omega = e^{2\pi i/3}$$

and obtain

$$\begin{aligned}\overline{q}_{3p}^{(3;p)} &= \prod_{j \in R_{3p}} (1 - r^{pj} - r^{3j}) = |(1-\omega^j)^p - 1|^2 \\ &= 3^p - (\omega^{-p} - \omega^p)(\omega - \omega^2)^p + 1 = 3 \ - \sigma 3^{(p+1)/2} + 1\end{aligned} \tag{2.20}$$

where $\sigma = (-3/p) = \pm 1$ is the quadratic character of $-3 \pmod{p}$. In particular, $\overline{q}_{15}^{(3;5)} = 3^5 + 3^3 + 1 = 271$ (see Table 2), and

$$\overline{q}_{21}^{(3;7)} = 2269, \ \overline{q}_{33}^{(3:11)} = 176419, \ q_{39}^{(3;13)} = 157 \cdot 10141. \tag{2.21}$$

To compute $q_{27}^{(\pm 9)}$, we note that the ninth roots of ω are r^{1+3k}. Hence,

$$\begin{aligned}q_{27}^{(\pm 9)} &= \prod_{k=1}^{9} |1 - r^9 - r^{\pm 1 + 3k}|^2 = |(1-\omega)^9 - \omega^{\pm 1}|^2 \\ &= 3^9 \pm 3^5 + 1 = 19684 \pm 243.\end{aligned} \tag{2.22}$$

3. THE FIBONACCI FACTORS OF d_n AND g_{2n}

Several extended principal factors of D_n are expressible as sums or ratios of Fibonacci numbers.

Theorem 3.1: For n odd, the factor $q_n^{(2)}$ of D_n is given by

$$q_n^{(2)} = F_{2n}/F_n = F_{n-1} + F_{n+1} = [\tau^n], \ \tau = (\sqrt{5}+1)/2 \tag{3.1}$$

where [ ] denotes the greatest integer function, and F_k denotes the kth Fibonacci number, defined by

$$F_0 = 0, \ F_1 = 1, \ F_{k+1} = F_k + F_{k-1}. \tag{3.2}$$

Proof: The roots of $z^2 - z - 1 = 0$ are $\tau = (\sqrt{5}+1)/2$ and $\overline{\tau} = -1/\tau$. Factorization of (2.11) for $u = 2$ and n odd yields

$$q_n^{(2)} = -\prod_{j=1}^{n} (1 - r^j\tau)(1 - r^j\overline{\tau}) = -(1-\tau^n)(1-\overline{\tau}^n) = \tau^n + \overline{\tau}^n = [\tau^n]. \tag{3.3}$$

It is known, and can be shown by induction, that

$$F_k = (\tau^k - \overline{\tau}^k)/(\tau - \overline{\tau}), \ F_{2k}/F_k = \tau^k + \overline{\tau}^k \tag{3.4a}$$

(3.4b) $\quad F_{k-1} + F_{k+1} = (\tau^{k-1} + \tau^{k+1} - \bar{\tau}^{k-1} - \bar{\tau}^{k+1})/(\tau - \bar{\tau}) = \tau^k + \bar{\tau}^k.$

Hence (3.3) and (3.4) imply (3.1).

The Fibonacci factors $[\tau^n] = q_n^{(2)}$ for the first 25 odd numbers $n = 10t + d$ follow, with factors underlined which are omitted from $\bar{q}_n^{(2)}$.

(3.5)

d \ $10t$	0	10	20	30	40
1	1	199	$\underline{2^2 \cdot 29} \cdot 211$	3010349	370248451
3	2^2	521	$139 \cdot 461$	$\underline{2^2 \cdot 199} \cdot 9901$	969323029
5	11	$\underline{2^2 \cdot 11} \cdot 31$	$\underline{11} \cdot 101 \cdot 151$	$\underline{11 \cdot 29} \cdot 71 \cdot 911$	$\underline{2^2 \cdot 11 \cdot 19 \cdot 31} \cdot 181 \cdot 541$
7	29	3591	$\underline{2^2 \cdot 19} \cdot 5779$	54018521	6643838879
9	$\underline{2^2} \cdot 19$	9349	$59 \cdot 19489$	$\underline{2^2 \cdot 521} \cdot 79 \cdot 859$	$29 \cdot 599786069$

Note that each prime factor of $\bar{q}_n^{(2)}$ (not underlined) is congruent to 1 (mod n).

Since d_n divides g_{2n} for odd n, so does F_{2n}/F_n.

Theorem 3.2: The integer g_{2n} is divisible by F_n for even n and by F_{2n}/F_n for odd n.

Proof: The product of the $[n/2] - 1$ factor pairs in (2.5) for which $j + k = n$ and $s = -1$ is expressible as

$$\prod_{0<2j<n} |s^j - s^{-j} - 1|^2 = \prod_{0<2j<n} (3 - s^{2j} - s^{-2j})$$

$$= \prod_{0<2j<n} (\tau + s^{2j}\bar{\tau})(\tau + s^{-2j}\bar{\tau}) \tag{3.6}$$

$$= (\tau^n - (-\bar{\tau})^n)/(\tau - (-1)^n\bar{\tau})$$

where $\tau + \bar{\tau} = -\tau\bar{\tau} = 1$. This is F_n for n even, and F_{2n}/F_n for n odd.

For $n = 2m$, the factors of (3.6) with j odd have product

$$(\tau^m + (-\bar{\tau})^m)/(\tau + (-1)^m\bar{\tau})$$

which divides k_{2m}. This product is F_m for m odd and F_{2m}/F_m for m even. So

$$3|k_4,\ 7|k_8,\ 5|k_{10},\ 13|k_{14},\ 47|k_{16},\ 123|k_{20},\ 89|k_{22}. \tag{3.7}$$

Theorem 3.3: If p is a prime > 5, then d_{5p} has the factor

$$\bar{q}_{5p}^{(5h)} = 1 + 5F_p(F_p - \sigma),\ \sigma = (p/5) = \pm 1,\ 5h \equiv 1 \pmod p \tag{3.8}$$

where F_p is the pth Fibonacci number and $\sigma = \pm 1$ is the quadratic character of p (mod 5).

Proof: Taking $r = e^{2\pi i/5p}$, $z = r^p$, $\tau^{-1} = z + z^{-1}$,

$$\begin{aligned} q_{5p}^{(5h)} &= \prod_{j \in R_{5p}} (1 - r^j - r^{5hj}) = \prod_{j \in R_{5p}} (r^{-5hj} - r^{(1-5h)j} - 1) \\ &= \prod_{j=1}^{4} (1 - (z^{2j} + 1)^p) = |1 - z^p\tau^{-p}|^2 |1 - z^{2p}(-\tau)^p|^2 \\ &= (\tau^p + \tau^{-p} - z^p - z^{-p})(\tau^p + \tau^{-p} + z^{2p} + z^{-2p}) \\ &= 5F_p(F_p - \sigma) + 1 \end{aligned} \tag{3.9}$$

since $\tau^p + \tau^{-p} = \sqrt{5}F_p$, $(z^1 + z^{-1})(z^2 + z^{-2}) = -1$, and

$$(z^p + z^{-p} - z^{2p} - z^{-2p})/\sqrt{5} = \sigma$$

is 1 if $p^2 \equiv 1 \pmod 5$ or -1 if $p^2 \equiv -1 \pmod 5$. The following such factors $q_{5p}^{(5h)}$ are prime except when $p = 13$

(3.10)

$5p$	15	35	55	65	85	95	115
$\overline{q}_{5p}^{(5h)}$	31	911	39161	131 • 2081	12360031	87382901	4106261531

Similarly, $181 | d_{45}$ and $21211 | d_{105}$.

4. POWER SUM FORMULAS FOR PRINCIPAL FACTORS OF D_n

The extended principal factors of $q_n^{(-1)} d_n$ in (2.2) or the corresponding factors $q_{n,c}^{(v:u)}$ of h_n in (2.7) may be treated together by defining

$$(c + 2)q_{n,c}^{(v:u)} = \prod_{j=1}^{n} |c + r^{vj} + r^{uj}|, \quad c = \pm 1, \quad r = e^{2\pi i/n} \tag{4.1}$$

when u, v are integers with $(u,v) = 1$ and $u > |v| > 0$.

Theorem 4.1: If z_k are the m roots of the equation

$$z^u + z^v + c = 0, \quad c = \pm 1, \quad u > |v| > 0 \tag{4.2}$$

where $m = u$ for $v > 0$ or $m = u - v$ for $v < 0$, then

$$\prod_{j=1}^{n} |c + r^{vj} + r^{uj}| = \prod_{k=1}^{m} |1 - z_k^n|. \tag{4.3}$$

Proof: Both sides of (4.3) equal the double product

$$\prod_{j=1}^{n} \prod_{k=1}^{m} |r^j - z_k|. \tag{4.4}$$

When $m = 2$, the two cases $(u,v) = (1,-1)$ and $(2,1)$ were involved in computing $q_n^{(-1)}$ in (2.3) with $z_k = -\omega, -\overline{\omega}$ and $q_n^{(2)}$ in (3.3) with $z_k = -\tau, -\overline{\tau}$. The factor $q_{n+}^{(2)}$ of h_n is 0 if $3|n$ or 1 otherwise, and may be omitted, since $3 \nmid n$.

The unexpected identities

$$(z^5 + z - 1) = (z + z^{-1} - 1)z(z^3 + z^2 - 1) \tag{4.5a}$$

$$(z^5 + z + 1) = (z^2 + z + 1)z(z^2 + z^{-1} - 1) \tag{4.5b}$$

enable us to write

(4.6) $$q_n^{(5)} = q_n^{(-1)} q_n^{(2:3)},\ q_{n+}^{(5)} = q_{n+}^{(2)} q_n^{(-2)} = q_n^{(-2)},$$

so the cubic cases $m = 3$ in (4.2) yield not only $q_{n+}^{(3)}$ and $q_n^{(3)}$ but also the two pairs of equal integral factors

$$q_n^{(5)}/q_n^{(-1)} = q_n^{(2:3)} \quad \text{and} \quad q_{n+}^{(5)} = q_n^{(-2)}.$$

Combining (4.1) and (4.3) for $m = 3$ yields

(4.7) $$(2 + c) \cdot q_{n,c}^{(v:u)} = |1 - s_{n,c}^{(v:u)} - \delta^n(1 - s_{-n,c}^{(v:u)})|,\quad \delta = \Pi z_k$$

where

(4.8) $$s_{n,c}^{(v:u)} = \sum_{k=1}^{m} z_k^n \quad \text{for} \quad z_k^u + z_k^v + c = 0.$$

The product $\delta = \Pi z_k$ is 1 for $q_n^{(3)}$ and $q_n^{(2:3)}$ and -1 for $q_{n+}^{(3)}$ or $q_n^{(-2)}$. We omit the subscript c when $c = -1$ and omit v when $v = 1$.

Replacement of z_k by $-1/z_k$ converts the roots z_k of $z^2 + z^{-1} - 1 = 0$ to those of $z^3 + z^2 - 1 = 0$, and replacement of z_k by $-z_k$ converts $z^3 + z + 1 = 0$ to $z^3 + z - 1 = 0$. Hence

(4.9) $$s_n^{(-2)} = (-1)\ s_{-n}^{(2:3)},\ s_{n+}^{(3)} = (-1)\ s_n^{(3)}.$$

Thus all six extended principal factors for $m = 3$ can be computed from the values of $s_n^{(2:3)}$ and $s_n^{(3)}$ for positive and negative n.

<u>*Theorem 4.2:*</u> The power sums $s_{n,c}^{(v:u)}$ satisfy the recurrence relations

(4.10) $$s_{n+u,c}^{(v:u)} + s_{n+v,c}^{(v:u)} + cs_{n,c}^{(v:u)} = 0.$$

<u>*Proof:*</u> Multiply $z_k^u + z_k^v + c = 0$ by z_k^n and sum over k.

Starting with the value $m = 3$ for $n = 0$, and the values $s_n^{(v:3)}$ for $n = \pm 1$, we obtain values where $v = 2$ or 1 as follows:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$s_n^{(2:3)}$	-1	1	2	-3	4	-2	-1	5	-7	6	-1	-6	12
$s_{-n}^{(2:3)}$	0	2	3	2	5	5	7	10	12	17	22	29	39
$s_n^{(3)}$	0	-2	3	2	-5	1	7	-6	-6	13	0	-19	13
$s_{-n}^{(3)}$	1	1	4	5	6	10	15	21	31	46	67	98	144

Using (4.7) and (4.9) we can then compute the three extended principal factors $q_n^{(-2)}$, $q_n^{(2:3)}$, and $q_n^{(3)}$ of d_n and the factor $q_{n+}^{(3)}$ of h_n or $k_{n/2}$. We use (4.6) to compute the additional factors $q_n^{(5)}$ and $q_{n+}^{(5)}$. We compute

$$\overline{q}_{n+}^{(v:u)} = \overline{f}_{n+}^{(y:x)}$$

by replacing $-c_{xj}$ by c_{xj} in Theorem 2.5. By (4.6) we write $\overline{q}_{n+}^{(5)} = \overline{q}_n^{(-2)}$. Then

$$h_7 = (\overline{q}_{7+}^{(3)})^{1/3} = 2,\ h_{11} = \overline{q}^{(-2)} = 23,$$
$$h_{13} = (\overline{q}_{13+}^{(-3)})^{1/3} = 53 \cdot 3,$$

(continued)

$$(4.14)\quad \begin{aligned} h_{17} &= \bar{q}_{17}^{(-2)}\bar{q}_{17+}^{(3)} = 103 \cdot 239 \\ h_{19} &= \bar{q}_{19}^{(-2)}\bar{q}_{19+}^{(3)}\left(\bar{q}_{19+}^{(3)}\right)^{1/3} = 191 \cdot 47 \cdot 7 \\ h_{23} &= \bar{q}_{23}^{(-2)}\bar{q}_{23+}^{(3)}\bar{q}_{23+}^{(-3)} = 691 \cdot 47^2 \cdot 829 \end{aligned}$$

Similarly, since $(2m - 1)^2 \equiv 1 \pmod{4m}$, the factor of k_n in (2.9) is not $\bar{q}_{n+}^{(n-1)}$ but its square root. Using $\bar{f}_{n+}^{(y;x)}$ as before, the factors k_n of D_{2n} for $2n < 44$ are

(4.15)

k_n	k_4	k_8	k_{10}	k_{14}	k_{16}	k_{20}
$(\bar{q}_{2n+}^{(n-1)})^{1/2}$	3	7	5	13	47	41
$\bar{q}_{2n}^{(-2)}$		17	5	2^3	97	281
$\bar{q}_{2n+}^{(3)}$		17	61	337	449	241
$\bar{q}_{2n+}^{(-3)}$			5	29	193	881
$\bar{q}_{2n+}^{(-5)}$			41	197	97	41
$\bar{q}_{2n+}^{(7)}$				113	353	281
$q_{2n+}^{(-7)}$				29	257	41

The remaining factors of k_{20} are

$$(4.16)\quad (\bar{q}_{40+}^{(9)}\bar{q}_{40+}^{(-9)}\bar{q}_{40+}^{(11)}\bar{q}_{40+}^{(-11)})^{1/2}\,\bar{q}_{40}^{(15)}\bar{q}_{40}^{(-15)} = 3^2 \cdot 31 \cdot 11 \cdot 41 \cdot 641 \cdot 41$$

Note that the factors $\bar{q}_{2n+}^{(u)}$ in (4.15) are congruent to their squares (mod $2n$). Factors of k_{22} are

$$(4.17)\quad \begin{aligned} k_{22} = {} & 67 \cdot 89 \cdot 353 \cdot 397 \cdot 419 \cdot 617 \cdot 661 \cdot 1013 \cdot 2113 \\ & 2333 \cdot 3257 \cdot 4357 \end{aligned}$$

The complete factorization of D_{44} is

$$(4.18)\quad D_{44} = -3(23 \cdot 89 \cdot 683)^3(5 \cdot 397 \cdot 2113)^3(d_{11}h_{11}k_{22})^6.$$

5. FINITE BINOMIAL SERIES FOR THE POWER SERIES OF ROOTS

The two sums $s_{n,b,c}^{(v:u)}$ and $s_{-n,b,c}^{(v:u)}$ of the nth and $-n$th powers of the u roots z of the trinomial equation

$$(5.2)\quad z^u + bz^v + bc = 0,\ b^2 = c^2 = 1,\ u > v > 0$$

can both be expressed as sums of a total of at most $2 + |n|/v(u - v)$ integers that involve binomial coefficients.

Theorem 6.1: The sum of the nth powers of the roots z_k of (5.1) is

$$(5.2a)\quad s_{n,b,c}^{(v:u)} = \sum_{0 \le j} \frac{n}{i}\binom{i}{j}(-b)^i c^{i-j},\ \text{where } ui - vj = n$$

$$(5.2b)\quad = \sum_{0 \le j} u\binom{i}{j} - v\binom{i-1}{j-1}(-b)^i c^{i-j},\ \text{where } ui - vj = n.$$

Proof: If we set $w_k = -bc$, then Equation (5.1) for z_k becomes

$$w_k^{-u} = (-bc)^{-1} = z_k^{-u}(1 + z_k^v/c), \tag{5.3}$$

which can be solved for z_k in terms of w_k by applying formula (3.5c) of [4], replacing the letters λ, μ, ν, c, q, k in [4] by $v' = u - v$, v, $-u$, w_k, n, j, respectively. Thus

$$z_k^n = \sum_{j=0}^{\infty} \frac{n}{jv + n}\binom{(jv + n)/u}{j} w_k^{jv+n} c^{-j}. \tag{5.4}$$

The sum of the u values of w_k^{jv+n} is $u(-bc)^i$ if $jv + n$ is an integral multiple ui of u, but is 0 otherwise. We obtain (5.2a) from (5.4) by setting $jv + n = ui$ and summing over j subject to this condition and $j \geq 0$. The equivalent form (5.2b) obtained by setting $n = ui - vj$ is clearly a sum of integers when $b^2 = c^2 = 1$. It also serves to assign the value $(-1)^j v$ to $\frac{n}{i}\binom{i}{j}$ when $i = 0$, $j = -n/v > 0$.

The conditions $j \geq 0$ and $(u - v)i/n + v(i - j)/n = 1$ in (5.2) imply $i/n \geq 0$, since $\binom{i}{j}$ vanishes for $0 < i < j$. Hence, $0 \leq j \leq i \leq n/(u - v)$ for $n > 0$, and $0 \leq j \leq j - i \leq -n/v$ for $n < 0$. Since successive j's differ in (6.2a) by u, there are at most $1 + n/u(u - v)$ terms for $n > 0$ and at most $1 + |n|/uv$ for $n < 0$. Both sums can be computed with at most $2 + |n|/v(u - v)$ terms.

The four sums in (4.11) and corresponding sums when $v = 1$ or $u - 1$ and $u > 3$ are expressible in terms of the following 4 simple nonnegative sums:

$$\sigma_0 = 1 + \sum_{0<k\leq n/u}'' \frac{n}{n - vk}\binom{n - vk}{k}, \quad \sigma_1 = \sum_{0<k\leq n/u}' \frac{n}{n - vk}\binom{n - vk}{k} \tag{5.5a}$$

$$\sigma_2 = \sum_{n/u\leq k\leq n/v}'' \frac{n}{k}\binom{k}{n - vk}, \qquad \sigma_3 = \sum_{n/u\leq k\leq n/v}' \frac{n}{k}\binom{k}{n - vk} \tag{5.5b}$$

where Σ'' and Σ' denote, respectively, the sums over even and odd k, and $u = v + 1$. Note that $\sigma_0 - 1$, σ_1, σ_2, and σ_3 are divisible by n when n is a prime.

Theorem 5.2: The 16 power sums $s_{m,b,c}^{(v:v+1)}$ and $s_{m,b,c}^{(v+1)}$ for $b^2 = c^2 = 1$, $m = \pm n$, are expressible for $n > 0$ in terms of the 4 binomial sums (5.5) as follows:

$$s_{n,b,c}^{(v:v+1)} = (-b)^n(\sigma_0 + (-b)^v c\sigma_1) \tag{5.6a}$$

$$s_{-n,b,c}^{(v:v+1)} = b^n(\sigma_2 - b^v c\sigma_3) \tag{5.6b}$$

$$s_{n,b,c}^{(v+1)} = c^n(\sigma_2 - c^v b\sigma_3) \tag{5.6c}$$

$$s_{-n,b,c}^{(v+1)} = (-c)^n(\sigma_0 - c^v b\sigma_1) \tag{5.6d}$$

Proof: For $n > 0$ and $u = v + 1$, we set $i - j = k$, $i = n - kv$ in (5.2a) and obtain

$$s_{n,b,c}^{(v:v+1)} = \sum_{0\leq k\leq n/u} \frac{n}{n - kv}\binom{n - kv}{k}(-b)^{n-kv}c^k. \tag{5.7}$$

Separating the sums for even and odd k, as in (5.5a), yields (5.6a). To obtain (5.6c), we replace v by 1 and u by $v + 1$, in (5.2a), and apply (5.5b). Then set $i = k$, $i - j = n - vk$, and separate terms for even and odd k. Replacing z_k by $1/z_k$ interchanges n and $-n$, b and c, v and $u - v$, taking $z^u + bz^b + bc = 0$ into $z^u + cz^{u-v} + bc = 0$, (5.6a) into (5.6d), and (5.6c) into (5.6b).

For $n = 7$, $v = 2$, we have

$$\text{(5.8)}\quad \begin{aligned} &\sigma_0(17) = 1 + \frac{17}{13}\binom{13}{2} + \frac{17}{9}\binom{9}{4} = 341; \quad \sigma_1(17) = \frac{17}{15}\binom{15}{1} + \frac{17}{11}\binom{11}{3} = 323; \\ &\sigma_2(17) = \frac{17}{6}\binom{6}{5} + \frac{17}{8}\binom{8}{1} = 34; \qquad \sigma_3(17) = \frac{17}{7}\binom{7}{3} = 85. \end{aligned}$$

To obtain the extended principal factors $q_n^{(-3)}$, $q_n^{(3:4)}$, $q_n^{(4)}$, and $q_{n+}^{(4)}$ related to quartic equations (4.2) or the 6 factors other than $q_n^{(5)}$ and $q_{n+}^{(5)}$ of (4.6) related to quintic equations, we apply Theorem 4.2 and express the sums $\Sigma(z_j z_k)^n$ for positive or negative n by $(s_n^2 - s_{2n})/2$. For the equation $z^4 + z^v + c = 0$ with $v = 1$ or 3 and $c = \pm 1$, we have $(z^4 + c)^2 = z^{2v}$, so g_{2n} satisfies the recurrence

$$\text{(5.9)}\qquad s_{8+2n} + 2cs_{4+2n} + s_{2n} = s_{2n+2v}.$$

We omit the details concerning the computation of these 10 extended factors —some of which may coincide with the two "quadratic" and six "cubic" factors described above. For higher degree than 5, the factors listed in Section 7 were computed by pocket calculator using (2.5).

6. THE MULTIPLICITY OF $p = 2n + 1$ IN D_n

The multiplicity of factors 23 in d_{11}, 59 in d_{29}, 83 in d_{41}, etc., as seen in Table 1, is clarified by the following theorem.

Theorem 6.1: If $p = 2n + 1$ is prime, then p^e divides D_n for some exponent $e \geq [(n - 1)/2]$.

Proof: If $\bar{s}$ is a primitive root (mod p), $1 < \bar{s} < 2n$, then $\bar{s}^{2n} \equiv 1$ (mod p) and the even powers $\bar{s}^{2j} = \bar{r}^j$ are quadratic residues which are nth roots of unity (mod p). A principal factor $\bar{q}_n^{(v:u)}$ of d_n will vanish (mod p) if and only if the congruence $s^{2jv} + s^{2ju} \equiv 1$ (mod p) holds for some j relatively prime to n. If $(v,u) = 1$, parametric solutions of this congruence are

$$\text{(6.1)}\qquad s^{jv} \equiv 2/(h' + h),\ s^{ju} \equiv (h' - h)/(h' + h) \text{ where } hh' \equiv 1 \pmod{p}.$$

There are $4[(n - 1)/2]$ admissible values of h, excluding $h^2 = \pm 1$ or 0, of which the four distinct values $\pm h$, $\pm h'$ yield the same ordered pair (s^{2jv}, s^{2ju}). Hence, there are $[(n - 1)/2]$ distinct ordered pairs of squares with sum 1 (mod p) and at least $[(n - 1)/2]$ factors p in D_n.

Note that the substitution of $(h \pm 1)/(h \mp 1)$ for h interchanges the squares s^{2jv} and s^{2ju}. If these squares are equal (mod p), each is 1/2, so 2 is a quadratic residue of p, p divides $2^n - 1$, $p \equiv \pm 1$ (mod 8), and $[(n - 1)/2]$ is odd. For example, 7 divides $2^3 - 1$, 17 divides $2^8 - 1$, 23 divides $2^{11} - 1$, etc. In any case, $[(n - 1)/4]$ factors p divide d_n. For example,

$$\text{(6.2)}\qquad 23^2 | d_{11},\quad 47^5 | d_{23},\quad 59^9 | d_{29},\quad 83^{10} | d_{41}$$

and the inequality $e \geq [(n - 1)/2]$ is exact except for $p = 59$ where

$$[(n - 1)/4] = 7 < e/2 = 9.$$

In this case we have

$$
\begin{aligned}
(6.3)\qquad 1 &\equiv 25 + 25^2 \equiv 15 + 15^5 \equiv 19 + 19^8 \equiv 3 + 3^{-11} \equiv 16^{-1} + 16^{13} \\
&\equiv 9 + 9^{-2} \equiv 17^{-1} + 17^2 \pmod{59}
\end{aligned}
$$

but three factors $q_{29}^{(u)}$ are 59^2, for $u = 5$ and -13 (or 3/2) as well as -2.

7. SUMMARY

We list all the principal factors $q_p^{(u)}$ of d_p for prime p in Table 1, defining u' so that $uu' \equiv 1 \pmod{p}$, and taking all u from 2 to $(p-1)/2$, except when $0 < u' < u$. We then replace $q_p^{(u)}$ by $q_p^{(-u)}$ on the list, and indicate by underlining that this has been done. However, in computing, we take $u = -2$ instead of $(p-1)/2$, and $u/v = 3/2$ instead of $u = (3-p)/2$, $(2 \pm p)/3$ or 5. Similarly, we can use the "quartic" factors with $u/v = -3$ or 4/3 instead of higher degree product formulas requiring more complicated calculations.

To find the prime factors of a large principal factor like

$$q_{47}^{(13)} = 10504313,$$

we assume a factorization $(1 + 94j)(1 + 94k)$ by Theorem 2.6, subtract 1, divide by 94, and get

$$(7.1)\qquad (1188)(94) + 76 = 94jk + j + k.$$

This implies $j + k = 76 + 282m$, and $jk = 1188 - 3m$ for some m. The only prime for $j < 7$ is 283, which does not divide $q_{47}^{(13)}$. Hence $j \geq 7$, and

$$j + k < 1188/7 + 7 < 177,$$

so $m = 0$. Thus, $j = 22$, $k = 54$, and $2069 \cdot 5077$ is the factorization.

For odd composite n, both $q_n^{(u)}$ and $q_n^{(-u)}$ may be listed as in (2.18) if u and n have a common factor, so we list them together in (7.3). Factors $q_{3p}^{(3:p)}$ in (2.21) must also be included in d_{3p} and factors like (3.8) in d_{5p}.

Factors of D_{4n+2} were given in (2.4), (2.7), and (4.14), whereas those of D_{4n} are obtained from (2.4), (2.9), and (4.15).

REFERENCES

1. P. Bachmann. *Das Fermatproblem in seiner bisherigen Entwicklung*. Berlin, 1919.
2. L. Carlitz. "A Determinant Connected with Fermat's Last Theorem." *Proc. A.M.S.* 10(1959):686-690.
3. L. Carlitz. "A Determinant Connected with Fermat's Last Theorem: Continued." *Proc. A.M.S.* 11 (1960):730-733.
4. J. S. Frame. "Power Series for Inverse Functions." *Amer. Math. Monthly* 64 (1957):236-240.
5. J. S. Frame. "Matrix Functions: A Powerful Tool." *Pi Mu Epsilon Journal* 6, No. 3 (1975):125-135.
6. E. Lehmer. "On a Resultant Connected with Fermat's Last Theorem." *Bull. A.M.S.* 41 (1935):864-867.
7. H. S. Vandiver. "Fermat's Last Theorem: Its History and the Nature of the Known Results Concerning It." *Amer. Math. Monthly* 53 (1946):555-578.
8. E. Wendt. "Arithmetische Studien über den 'letzen' Fermatschen Satz, welcher aussagt, dass die Gleichung $a^n = b^n + c^n$ für $n > 2$ in ganzen Zahlen nicht auflosbar ist." *J. für reine und angew. Math.* 113 (1894): 335-347.

*****