ON THE INTEGRAL DIVISORS OF $a^n - b^n$

By Geo. D. Birkhoff and H. S. Vandiver*

The object of the following discussion is to develop some of the arithmetical properties of the divisors of $a^n - b^n$, and of forms related to it, in an elementary way. We have endeavored to give natural and concise proofs of the known theorems (I, II, III and IV) which lead up to the enunciation and proof of a new proposition (V). It is also shown that a principle in the theory of cyclotomic divisors may be used in giving a very simple proof of the irreducibility of $X^{p-1} + X^{p-2} + \cdots + 1$, p being a prime integer. All the numbers considered will be positive integers.

1. General Properties of the Cyclotomic Divisors. If a is greater than b and prime to it we write

$$V_n = a^n - b^n.$$

If $1, n', n'', n'''$, etc. are all the different divisors of n which are less than n, then V_n is divisible by $V_1, V_{n'}, V_{n''}, \cdots$, etc. A divisor of V_n which is prime to all these numbers is termed a *primitive divisor* of the form. Thus 5 is a primitive divisor of $2^4 - 1$. Other divisors are called *imprimitive*, and we may regard unity as a primitive divisor of any V.†

A characteristic property of primitive divisors is given by the following

Theorem I (Euler). *Any primitive divisor of V_n is of the form* $1 \pmod{n}$.

If unity is the only existing primitive divisor, the theorem holds. If others

* The principal results in the present article were included in a communication made to the American Mathematical Society, at the meeting held Dec. 29, 1902. The authors are indebted to Professor E. S. Crawley and Dr. G. H. Hallett, of the University of Pennsylvania for several suggestions.

† In the classification of divisors of V_n the term *proper divisor* is employed by many writers, being defined as a factor which does not divide any of the forms $V_1, V_{n'}, V_{n''}$, etc. For examples, see Serret, *Cours d'algèbre supérieure* 5th edition, vol. 2, p. 145, and Dickson's *Linear Groups*, p. 20. According to this definition prime primitive divisors are prime proper divisors, and it is not difficult to see that the theory of proper divisors depends upon that of primitive divisors.

exist, let p be any prime one, and determine m from the congruence $a \equiv bm \pmod{p}$; then $V_n \equiv b^n m^m - b^n \equiv 0 \pmod{p}$ and since b is prime to p, $m^n - 1 \equiv 0 \pmod{p}$. It now follows from the definition of p, that m appertains to n, modulo p, so that $p - 1 \equiv 0 \pmod{n}$ or $p \equiv 1 \pmod{n}$, showing that any such prime divisor has the form 1 (mod n). Now any composite primitive divisor of V_n is the product of prime divisors of the same type. For if there is a divisor of the composite which is not primitive then the composite cannot be prime to V_1, $V_{n'}$, $V_{n''}$, etc., where 1, n', n'', etc., have the same meaning as before. Hence all the primitive divisors are of the form 1 (mod n), and the theorem is proved.

Before proceeding with the further study of primitive divisors we must consider the two following theorems:

THEOREM II. *If V_1 is prime to n, then V_n/V_1 is prime to V_1.*

THEOREM III. *If p is prime and V_1/p^k is an integer prime to p, then V_p is divisible by p^{k+1}; it is not divisible by p^{k+2}, except when $V_1 = 2M$, where M is odd, in which case V_2 may be divisible by any power of 2 greater than 4.*

To prove Theorem II, we have

$$V_1 = a - b,$$

and
$$a^n = (b + V_1)^n = b^n + nb^{n-1} V_1 + \frac{n(n-1)}{2!} b^{n-2} V_1^2 + \cdots,$$

or
$$a^n - b^n = V_n = V_1\left(nb^{n-1} + \frac{n(n-1)}{2!} b^{n-2} V_1 + \cdots + V_1^{n-1}\right),$$

whence
$$\frac{V_n}{V_1} \equiv nb^{n-1} \pmod{V_1}.$$

Now b is prime to V_1; therefore if n is prime to V_1, then V_n/V_1 is also.

To prove Theorem III put $V_1/p^k = M$, an integer prime to p, and suppose first, that p is an odd prime. Then

$$V_1 = a - b = Mp^k,$$

from which

$$\begin{aligned} a^p &= (b + Mp^k)^p \\ &= b^p + p^{k+1} b^{p-1} M + \cdots + p^{pk} M^p; \end{aligned}$$

or, since p is prime,

$$a^p - b^p = V_p = p^{k+1}\left(b^{p-1}M + \frac{p^k(p-1)}{2!}b^{p-2}M^2 + \cdots + p^{k(p-1)-1}M^p\right),$$

whence, p being odd,

$$\frac{V_p}{p^{k+1}} \equiv b^{p-1}M \pmod{p}.$$

It then follows that V_p/p^{k+1} is prime to p, since b and M are.

If we have $V_1/2^k = M_1$ say, where M_1 is odd and $k > 1$, then we find (as above) that V_2 is divisible by 2^{k+1} but not by 2^{k+2}. But in the case $k = 1$, we have

$$V_1 = a - b = 2M_1 \text{ and } V_2 = 4(bM_1 + M_1^2).$$

Then, since b and M are odd, V_2 is divisible by 8, or by a higher power of 2. This completes the proof of Theorem III.

We now resume the consideration of primitive divisors. Let the resolution of V_n into its distinct prime factors be

$$V_n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}.$$

If p_c, p_d, p_e, etc. are all the distinct prime primitive divisors of V_n, consider the product

$$P(n) = p_c^{a_c}p_d^{a_d}p_e^{a_e}\cdots$$

This number $P(n)$ shall be termed the *arithmetic primitive factor* of V_n, and is evidently divisible by any primitive divisor of V_n. Thus 5^2 or 25 is the arithmetical primitive factor of $7^4 - 1$, the primitive divisors being 1, 5 and 25. Similarly, unity is the arithmetical primitive factor of $2^6 - 1$.

The number $P(n)$ is closely related to a certain algebraic factor of V_n. We define this function by

$$F(n) = \frac{V_n \Pi V_{\frac{n}{pq}} \Pi V_{\frac{n}{pqr}} \cdots}{\Pi V_{\frac{n}{p}} \Pi V_{\frac{n}{pqr}} \cdots} \tag{1}$$

where p, q, r, s, etc. are the distinct prime divisors of n,

$$\Pi V_{\frac{n}{p}} = V_{\frac{n}{p}}\ V_{\frac{n}{q}}\ V_{\frac{n}{r}} \cdots,$$

$$\Pi V_{\frac{n}{pq}} = V_{\frac{n}{pq}}\ V_{\frac{n}{pr}}\ V_{\frac{n}{qr}}\ V_{\frac{n}{ps}} \cdots,$$

and similarly for the other products. In the numerator of (1), the indices of

the binomials are formed through the division of n by an even number of prime factors; in the denominator they are formed through the division by an odd number.

The form $F(n)$ has the following property:

$$V_n = F(1)F(n)F(n')F(n'') \cdots,$$

where 1, n, n', n'', etc. are all the distinct divisors of n. This function may also be defined by the equation

$$F(n) = (a - \omega_1 b)(a - \omega_2 b) \cdots (a - \omega_{\phi(n)} b)$$

($\omega_1, \omega_2, \cdots \omega_{\phi(n)}$, being the $\phi(n)$ primitive roots of $x^n - 1 = 0$), and can be conveniently termed the *algebraic primitive factor* of V_n, since it has no *algebraic* factor in common with V_1, $V_{n'}$, $V_{n''}$, etc.*

Let λ be a quantity defined by the relation

$$F(n) = \lambda P(n).$$

For the determination of λ we have,

THEOREM IV.† *If $n \neq 2$, then $\lambda = 1$, unless $P(n/p^a) \equiv 0 \pmod{p}$, n/p^a being an integer prime to p. In the latter case, $\lambda = p$.*

From the equation

$$V_n = F(1)\ F(n)\ F(n')\ F(n'')\ \cdots$$

we get

$$V_n / V_{\frac{n}{t}} \equiv 0 [\text{mod } F(n)],$$

where t is any divisor of n exclusive of unity. Taken in connection with Theorem II, this relation shows that $F(n)$ is prime to every imprimitive divisor of V_n which is prime to n, hence if we have $F(n) = \lambda P(n)$, λ is an integer each of whose prime factors must divide n. Suppose p is such a prime factor. From equation (1) we have immediately, writing $F(a,b,n)$ for the algebraic primitive factor of $a^n - b^n$,

$$F(a, b, n) = \frac{F(a^{p^a}, b^{p^a}, n')}{F(a^{p^{a-1}}, b^{p^{a-1}}, n')}$$

* For the proofs of the foregoing relations see Bachmann's *Kreistheilung*, 1872, pp. 13–17. Notice that $\phi(n)$ means, as usual, the number of integers less than and prime to n.

† The first enunciation of this theorem, in its complete form, appears to be that of Sylvester, *American Journal Math.* vol. 2 (1879), p. 365. His demonstration is different from the one given here.

where $n = p^a n'$, and n' is prime to p. Applying the relation*

$$F(a^{p^t}, b^{p^t} n') \equiv [F(a, b, n')]^{p^t} \pmod{p},$$

we obtain

$$F(a, b, n) \equiv [F(a, b, n')]^{p^{a-1}(p-1)} \pmod{p}.$$

This shows that $F(a,b,n) \equiv 0 \pmod{p}$ only when $F(a,b,n') \equiv 0 \pmod{p}$. If the latter congruence is not satisfied for any p, then $F(n) = P(n)$. But if it is satisfied, then since $F(n')/P(n') = \lambda'$ is prime to p, p is also a divisor of $P(n')$, and is of the form $1 \pmod{n'}$. This gives $p > n/p^a$, hence p is uniquely determined as the largest prime dividing n, and we must have $\lambda = p^A$, where A is to be determined.

It can be shown that if $n > 2$, then $A = 1$. The only V in the denominator of the expression for $F(n)$ given in (1) which contains p is $V_{\frac{n}{p}}$, and in the numerator p divides V_n only, there being none other of the binomials in $F(n)$ having $F(a, b, n')$ as a factor. If $V_{\frac{n}{p}} = p^m K$, then $V_n = p^{m+1} K'$, where K and K' are prime to P, and $n > 2$ (Theorem III). Hence $F(n)$ is divisible by p but not by p^2 (for $n > 2$) and the theorem follows.

As a useful special case of theorem IV, we have :—

If p is prime, then $F(p) = \dfrac{a^p - b^p}{a - b}$, *and* $F(p) = pP(p)$ *or* $P(p)$ *according as $a - b$ is or is not congruent to zero, modulo p.*

The foregoing theorems enable us to demonstrate the following interesting proposition regarding the primitive divisors of V_n :—

THEOREM V. *If $n \neq 2$, then any form V_n possesses at least one primitive divisor* (other then unity), *with the single exception* $V_n = 2^6 - 1^6$.

To prove this, it is sufficient to show that $P(n) > 1$. We consider first the case in which $P(n) = \dfrac{F(n)}{p}$, where, as in Theorem IV, $n = p^a n'$, $p \equiv 1 \pmod{n'}$, and $F(n') \equiv 0 \pmod{p}$.

Since $F(n')$ is not zero, we have

$$F(n') \geqq p,$$

from the relation $F(n') \equiv 0 \pmod{p}$;

---

* See Serret's *Cours d'algèbre supérieure*, 5th Edition, vol. 2, p. 134.

and therefore $$P(n) \geqq \frac{F(n)}{F(n')}.$$

Suppose, for the present, $n' \neq 1$.

Since a and b are integers, and $a > b$, we have

$$\begin{aligned} a^k - b^k &= (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}) \\ &\geqq a^{k-1} + a^{k-2}b + \cdots + b^{k-1}, \\ a^k - b^k &> a^{k-1}. \end{aligned}$$

Applying this inequality to the numerator of the expression for $F(n)$ in (1), we find

$$V_n \prod_{pq} V_{\frac{n}{pq}} \prod_{pqrs} V_{\frac{n}{pqrs}} \cdots > a^{n-1} \prod a^{\frac{n}{pq}-1} \prod a^{\frac{n}{pqrs}-1} \cdots,$$

where $$\prod a^{\frac{n}{pq}-1} = a^{\frac{n}{pq}-1} \cdot a^{\frac{n}{pr}-1} \cdot a^{\frac{n}{ps}-1} \cdots,$$

and similarly for the other products. Then,

$$\begin{aligned} V_n \prod_{pq} V_{\frac{n}{pq}} \prod_{pqrs} V_{\frac{n}{pqrs}} \cdots &> a^{n-1+\Sigma\left(\frac{n}{pq}-1\right)+\Sigma\left(\frac{n}{pqrs}-1\right)\cdots}, \\ &> a^{-2^m-1+n+\Sigma\frac{n}{pq}+\Sigma\frac{n}{pqrs}\cdots}, \end{aligned}$$

where m is the number of distinct prime factors in n.

For the denominator of $F(n)$ we have, since $a^k - b^k < a^k$,

$$\prod_{p} V_{\frac{n}{p}} \prod_{pqr} V_{\frac{n}{pqr}} \cdots < a^{\Sigma\frac{n}{p}+\Sigma\frac{n}{pqr}\cdots},$$

and by division of the inequalities for numerator and denominator of (1), and using the relation

$$\phi(n) = n - \Sigma\tfrac{n}{p} + \Sigma\tfrac{n}{pq} - \Sigma\tfrac{n}{pqr} + \cdots,$$

we obtain

$$F(n) > a^{\phi(n)-2^m-1}.$$

Now by applying the inequality $a^k - b^k < a^k$ to the numerator of $F(n')$ and $a^k - b^k > a^{k-1}$ to the denominator, we obtain

$$F(n') < a^{\phi(n')-2^{m-2}},$$

m, by hypothesis, not being unity. Hence

$$\frac{F(n)}{F(n')} > a^{\phi(n) - \phi(n') - 3 \cdot 2^{m-2}}.$$

Consider the expression $\phi(n) - \phi(n') - 3 \cdot 2^{m-2}$. Since $n' > 1$, we have $\phi(n') \geqq 2^{m-2}$. Also, $p^{a-1}(p-1) - 1 \geqq 3$, except when $p = 3$, noting that $p \neq 2$. Therefore

$$\phi(n')[p^{a-1}(p-1) - 1] \geqq 3 \cdot 2^{m-2},$$

or

$$\phi(n) - \phi(n') - 3 \cdot 2^{m-2} \geqq 0,$$

except when $p = 3$, that is, except when $n = 6$. Hence

$$\frac{F(n)}{F(n')} > 1, \text{ or } P(n) > 1,$$

except when $n = 6$. We have $F'(6) = a^2 - ab + b^2$, which is greater than 3 except for $a = 2$, $b = 1$, in which case the arithmetical primitive factor is unity and no primitive divisor other than unity exists.

When $n' = 1$, then $n = p^a$ and from (1) $F(p^a) = \dfrac{V_n}{V_{\frac{n}{p}}}$, which expression is greater than p since the expanded forms contain p positive integral terms some of which are greater than unity. Hence $P(p^a) > 1$. The case $P(n) = F(n)$ remains to be disposed of. We have $F(n) > a^{\phi(n) - 2^{m-1}}$. Now obviously $\phi(n) \geqq 2^{m-1}$, hence $F(n) > 1$ and $P(n) > 1$. Theorem V is therefore completely proved. An immediate consequence of Theorem V is the following:—

Any form $a^n - b^n$ possesses at least one divisor of the form $1 \pmod{n}$, *other than unity.*

2. Applications of the Theory.

1. *There is an infinity of primes of the form* $1 \pmod{n}$.

Consider the infinite series

$$P(n),\ P(2n),\ P(3n),\ \cdots\ P(kn)\ \cdots.$$

The integers thus represented are all relatively prime and by Theorem V each contains at least one prime divisor of the form $1 \pmod{n}$. Consequently

the series furnishes an infinity of distinct primes of this form.*

2. *The function $F(p)$ is irreducible in the domain of real integers, p being prime.*†

Proof. Put $b = 1$, and suppose

$$F(p) = \frac{a^p - 1}{a - 1}$$

reducible; then

$$\frac{a^p - 1}{a - 1} = a^{p-1} + a^{p-2} + \cdots + 1 = f_1(a) f_2(a),$$

where $f_1(a)$ and $f_2(a)$ are polynomials in a, with integral coefficients.‡

In the above identity give a the values $0, 2, 3, 4, \cdots, p-1$. The special case of Theorem IV (already mentioned) gives for any of these values

$$F(p) = P(p),$$

and also $f_1(a) \equiv 1 \pmod{p}$, since it is a divisor of $P(p)$. Consequently the congruence $f_1(a) - 1 \equiv 0 \pmod{p}$ admits $p - 1$ roots, which is impossible since p is prime, and the degree of $f_1(a)$ is less than $p - 1$. $F(p)$ is therefore irreducible.

---

*Evidently Theorem V is not necessary for the demonstration of this proposition, as a proof can be deduced from Theorem IV alone. In this latter form the proof has been given by a number of writers. For examples, see Kronecker, *Vorlesungen über Zahlentheorie*, pp. 440-441; Hilbert, *Algebraische Zahlkörper*, p. 334; Sylvester, *Comptes rendus*, vol. 104, pp. 1085-86.

†For other proofs of this theorem, see the references in H. J. Smith's *Report on the Theory of Numbers*, Works, vol. I, p. 127, footnote.

‡ *Cf.* a theorem of Gauss's; *Disquisitiones arithmeticae*, Art. 341.