ON DIVISIBILITY BY $\frac{a^k - b^k}{a - b}$

A. SCHINZEL

ABSTRACT. The recent result of F. Luca on divisibility by $g^k - 1$ is extended to divisibility by $(a^k - b^k)/(a - b)$, where $a > b$ are positive integers.

F. Luca [1] has recently proved the following theorem.

If a, k, and n are positive integers, c_j are non-negative integers, not all zero, and

$$\sum_{i=0}^{k-1} a^i \,\Big|\, \sum_{j=0}^{n-1} c_j a^j,$$

then

$$k \le \sum_{j=0}^{n-1} c_j.$$

A stronger inequality under the same assumption has been obtained by H. Pan [2]. Luca's theorem will be generalized as follows.

Theorem 1. *If a, b, k, and n are positive integers, $a > b$, $(a, b) = 1$, c_j are non-negative integers, not all zero, and*

$$\sum_{i=0}^{k-1} a^i b^{k-1-i} \,\Big|\, \sum_{j=0}^{n-1} c_j a^j b^{n-1-j}, \tag{1}$$

then $k \le \sum_{j=0}^{n-1} c_j$.

Proof. It follows from (1) that for every integer $i \in [0, k)$

$$\frac{a^k - b^k}{a - b} \,\Big|\, \sum_{j=0}^{n-1} c_j a^{j+i} b^{n+k-2-i-j}.$$

Since for all non-negative integers $i < k$, $j < n$

$$a^{j+i} b^{n+k-2-i-j} \equiv a^{k\left\{\frac{j+i}{k}\right\}} b^{n+k-2-k\left\{\frac{j+i}{k}\right\}} \pmod{a^k - b^k},$$

we obtain

$$\frac{a^k - b^k}{a - b} \,\Big|\, b^{n-1} \sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}}.$$

Since $\left(\frac{a^k - b^k}{a - b}, b\right) = 1$, it follows that

$$\frac{a^k - b^k}{a - b} \,\Big|\, \sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} \quad (i = 0, 1, \ldots, k-1)$$

and since the above sum is positive

$$\frac{a^k-b^k}{a-b} \le \sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} \quad (i=0,1,\dots,k-1).$$

Since $k\{(j+i)/k\}$ runs through the complete set $\{0,1,\dots,k-1\}$ as i runs through $\{0,1,\dots,k-1\}$, summing over all $i<k$ we obtain

$$k\frac{a^k-b^k}{a-b} \le \sum_{j=0}^{n-1} c_j \frac{a^k-b^k}{a-b}, \quad \text{hence,} \quad k \le \sum_{j=0}^{n-1} c_j.$$

Theorem 1 ceases to be true, if the condition $a>b>0$ is replaced by $a>|b|>0$, as shown by counterexamples □

1. $\sum_{j=0}^{n-1} c_j x^j = (-bx+a)\sum_{j=0}^{n-2} d_j x^j$, d_j integers, $k>(a-b)\sum_{j=0}^{n-2} d_j$. (Note that here $\sum_{j=0}^{n-1} c_j a^j b^{n-1-j} = 0$).
2. $a+b=\pm 1$, k even, $n=k-1$, $c_j=1$ (j even), $c_j=0$ (j odd),

which example 2 can be modified by multiplying the right-hand side of (1) by $a^l b^m$.

The computation kindly performed by Dr. M. Ulas in the range $a\le 10$, $n=3$ or 4, $k\le 6$; $n=5$ or 6, $k\le 8$ under the assumption $\sum_{j=0}^{n-1} c_j < k$ produced only examples with $a-b \mid \sum_{j=0}^{n-1} c_j$, or $\sum_{j=0}^{n-1} c_j \ge k/2$. On the other hand, we only have the following theorems.

Theorem 2. *If $a>|b|>0$, $(a,b)=1$, and c_j are integers, not all zero, and* (1) *holds, then either*

$$a-b \,\Big|\, \sum_{j=0}^{n-1} c_j \Big/ (c_0,\dots,c_{n-1}), \quad \textit{or} \quad \sum_{j=0}^{n-1} |c_j| \ge k\frac{a^k-b^k}{a^k-|b|^k}\cdot\frac{a-|b|}{a-b}.$$

Theorem 3. *If $a>|b|>0$, $(a,b)=1$, c_j are integers, not all zero, and* (1) *holds, then*

$$(k,a-b) \,\Big|\, \sum_{j=0}^{n-1} c_j \tag{2}$$

and either

$$\frac{\operatorname{rad} k}{(\operatorname{rad} k, 2)} \,\Big|\, \sum_{j=0}^{n-1} c_j \Big/ (c_0,\dots,c_{n-1}), \tag{3}$$

or

$$\sum_{j=0}^{n-1} |c_j| > \max\left\{a-|b|, \frac{a+|b|}{2}\right\}. \tag{4}$$

Here $\operatorname{rad} k = \prod_{p\mid k,\, p\ prime} p$.

The proof is based on several lemmas.

Lemma 1. *If under the assumptions of Theorem 2 for a certain i*

$$\sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} = 0, \tag{5}$$

then

$$a-b \,\Big|\, \sum_{j=0}^{n-1} c_j \Big/ (c_0, \ldots, c_{n-1}).$$

Proof. It follows from (5) that

$$\sum_{j=0}^{n-1} c_j \left(\frac{a}{b}\right)^{k\left\{\frac{j+i}{k}\right\}} = 0.$$

Thus, $f(x) := \sum_{j=0}^{n-1} c_j x^{k\left\{\frac{j+i}{k}\right\}}$ has a zero at $\frac{a}{b}$, and by Bézout's Theorem

$$f(x) = (-bx+a)g(x),$$

where $g \in \mathbb{Q}[x]$. However, $(a,b)=1$, hence by Gauss's Theorem,

$$C(f) = C(g),$$

when $C(f)$, $C(g)$ are, respectively, the content of f and g. Therefore,

$$C(f)^{-1} \sum_{j=0}^{n-1} c_j = C(f)^{-1} f(1) = (a-b) C(g)^{-1} g(1)$$

and since $(c_0, \ldots, c_{n-1}) \mid C(f)$, $C(g) \mid g(1)$, the lemma follows. □

Proof of Theorem 2. Arguing as in the proof of Theorem 1, we infer that

$$\frac{a^k - b^k}{a-b} \,\Bigg|\, \sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} \quad (i = 0, \ldots, k-1). \tag{6}$$

If, for a certain $i < k$, the right-hand side of (6) is 0, we have by the lemma

$$a-b \,\Big|\, \sum_{j=0}^{n-1} c_j / (c_0, \ldots, c_{n-1}).$$

If, for each $i < k$, the right-hand side of (6) is not 0, then for a certain $\varepsilon_i \in \{1, -1\}$ we have

$$\varepsilon_i \sum_{j=0}^{n-1} c_j a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} \geq \frac{a^k - b^k}{a-b} \quad (i = 0, \ldots, k-1).$$

Summing over all i and using for every j

$$\sum_{i=0}^{k-1} \varepsilon_i a^{k\left\{\frac{j+i}{k}\right\}} b^{k-1-k\left\{\frac{j+i}{k}\right\}} \leq \frac{a^k - |b|^k}{a - |b|},$$

we obtain

$$\sum_{j=0}^{n-1} c_j \geq k \cdot \frac{a^k - b^k}{a^k - |b|^k} \cdot \frac{a - |b|}{a-b},$$

which completes the proof. □

Note that the right-hand side in always at least $k\frac{a-|b|}{a-b}$.

Remark. *The proofs of Theorems 1 and 2 show that if* (1) *is replaced by divisibility*

$$d \,\Big|\, \sum_{j=0}^{n-1} c_j a^j b^{n-1-j}, \qquad \text{where } d \,|\, a^k - b^k,$$

then under the other assumptions of the relevant theorem

$$kd\frac{a-b}{a^k-b^k} \le \sum_{j=0}^{n-1} c_j,$$

or either

$$a - b \,\Big|\, \sum_{j=0}^{n-1} c_j/(c_0, \dots, c_{n-1}),$$

or

$$\sum_{j=0}^{n-1} |c_j| \ge kd\frac{a-|b|}{a^k-|b|^k},$$

respectively.

Lemma 2. *If ζ_p is a primitive root of unity of prime order p, c_j are integers and*

$$\sum_{j=0}^{n-1} c_j \zeta_p^j = 0, \tag{7}$$

then

$$p \,\Big|\, \sum_{j=0}^{n-1} c_j/(c_0, \dots, c_{n-1}).$$

Proof. Let $f(x) = \sum_{j=0}^{n-1} c_j x^j$, $\phi_p(x) = 1 + x + \cdots + x^{p-1}$. Since $\phi_p(\zeta_p) = 0$ and ϕ_p is monic and irreducible over $\mathbb{Q}$, it follows from (7) that $f = \phi_p g$, where $g \in \mathbb{Z}[x]$. By Gauss's Theorem

$$C(f) = C(g)$$

and

$$\sum_{j=0}^{n-1} c_j/(c_0, \dots, c_{n-1}) = C(f)^{-1} f(1) = C(g)^{-1}\phi_p(1) g(1) = pC(g)^{-1} g(1).$$

Since $C(g)^{-1} g(1) \in \mathbb{Z}$, the lemma follows. □

Lemma 3. *If $a > |b| > 0$, p is an odd prime, then*

$$\frac{a^p - b^p}{a - b} > \max\left\{a - |b|, \frac{a+|b|}{2}\right\}^{p-1}. \tag{8}$$

Proof. If $b > 0$, (8) follows at once from the inequality for $\phi_\nu(A, B)$ proved for $\nu > 1$, A, B positive in Section 3 of [3]. If $b < 0$ we have

$$\frac{a^p - b^p}{a - b} = \phi_{2p}(a, |b|)$$

and since $\varphi(2p) = p - 1$ the same inequality applies. □

A short *ad hoc* proof is also possible.

Proof of Theorem 3. We have

$$\frac{a^k - b^k}{a-b} = \sum_{i=0}^{k-1} a^i b^{k-1-i} \equiv k b^{k-1} \equiv 0 \pmod{k, a-b}$$

and

$$\sum_{j=0}^{n-1} c_j a^j b^{n-1-j} \equiv b^{n-1} \sum_{j=0}^{n-1} c_j \pmod{k, a-b}$$

and, since $(a, b) = 1$, (2) follows from (1).

If, for all odd prime factors of k, (7) holds, then by Lemma 2, (3) holds.

If, for a certain odd prime factor p of k,

$$\alpha = \sum_{j=0}^{n-1} c_j \zeta_p^j \neq 0,$$

then

$$N\alpha \leq \left(\sum_{j=0}^{n-1} |c_j| \right)^{p-1}, \tag{9}$$

where $N\alpha$ is the norm of α from $\mathbb{Q}(\zeta_p)$ to $\mathbb{Q}$. On the other hand, by (1)

$$a - b\zeta_p \,\Big|\, \sum_{j=0}^{n-1} c_j a^j b^{n-1-j},$$

hence,

$$a - b\zeta_p \,\Big|\, b^{n-1} \sum_{j=0}^{n-1} c_j \zeta_p^j$$

and, since $(a, b) = 1$,

$$a - b\zeta_p \mid \alpha$$

and, by Lemma 3 and the fact that $\alpha \neq 0$,

$$N\alpha \geq N(a - b\zeta_p) = \frac{a^p - b^p}{a-b} > \max\left\{ a - |b|, \frac{a + |b|}{2} \right\}^{p-1}. \tag{10}$$

Now, (4) follows from (9) and (10). □

Note. Computations made by A. Zabłocki for $k, n < 16$ did not discover any example of divisibility (1) with $16 > a > -b > 0$, $(a, b) = 1$ and the sum of nonnegative c_j nondivisible by $a - b$ and less than $k/2$.

Acknowledgement

Thanks are due to the referee for his suggestions incorporated in the paper.

References

[1] F. Luca, *On a problem of Bednarek*, Comm. Math., (to appear).
[2] H. Pan, *On the m-ary expansion of a multiple of* $(m^k - 1)/(m - 1)$, Publ. Math. Debrecen, (to appear).
[3] A. Schinzel, *On primitive prime factors of* $a^n - b^n$, Proc. Cambridge Philos. Soc., **58** (1962), 555–562, see also Selecta, Vol. 2, 1036–1045.

MSC2010: 11A07, 11R18.

Institute of Mathematics, Polish Academy of Sciences, Śniadeckich 8, 00-956 Warsaw, Poland
E-mail address: schinzel@impan.pl