

WHEN  $a^r - b^r$  DIVIDES  $(a - b)^s$

William H. Wilson

In this paper we answer a number-theoretic question which has applications in group theory.

**PROPOSITION.** *If  $a$  and  $b$  are coprime and  $r$  is a prime number, then  $a^r - b^r$  divides a power of  $a - b$  if and only if  $r = 2$  and  $a$  is of the form  $2^t - b$ .*

*Proof.* We may suppose that  $a \geq b$ . If  $a - b = 0$  or  $1$ , it is easy to see that the proposition is true. Thus we may suppose that  $a - b \geq 2$ , and let  $a - b = q_1 q_2 \dots q_d$  be the prime decomposition of  $a - b$ . Then

$$\begin{aligned} a^r - b^r &= \sum_{i=1}^r \binom{r}{i} q_1^i \dots q_d^i b^{r-i}, \text{ by the binomial theorem,} \\ &= q_1 \dots q_d \left\{ rb^{r-1} + q_1 \dots q_d \left[ \binom{r}{2} b^{r-2} + \dots + q_1^{r-2} \dots q_d^{r-2} \right] \right\} \\ (1) \quad &= q_1 \dots q_d \{ rb^{r-1} + q_1 \dots q_d M \}, \text{ say.} \end{aligned}$$

Now  $a^r - b^r$  divides a power of  $a - b$  if and only if the prime factors of  $a^r - b^r$  lie in  $\{q_1, \dots, q_d\}$ .

If  $r \notin \{q_1, \dots, q_d\}$ , then  $rb^{r-1}$  is coprime to each  $q_i$  so no  $q_i$  can divide  $rb^{r-1} + q_1 \dots q_d M$ . Hence, by equation (1),  $a^r - b^r$  has a prime factor not in  $\{q_1, \dots, q_d\}$ . If, on the other hand,  $r \in \{q_1, \dots, q_d\}$ , then we may assume that  $r = q_1$ , say, so that

$$rb^{r-1} + q_1 q_2 \dots q_d M = r(b^{r-1} + q_2 \dots q_d M).$$

In this case, either  $b^{r-1} + q_2 \dots q_d M$  has a prime factor not in  $\{q_1, \dots, q_d\}$ , or else  $b^{r-1} + q_2 \dots q_d M$  is a power of  $r = q_1$ , so that by equation (1),  $a^r - b^r = q_1 \dots q_d r^t$ , or

$$(2) \quad (a^r - b^r)/(a - b) = a^{r-1} + a^{r-2} b + \dots + b^{r-1} = r^t$$

for some  $t$ . If  $t = 1$ , then  $a = b = 1$ , contradicting  $a - b \geq 2$ , so

we can assume that  $t \geq 2$ . Writing  $a - b = hr$  and using the binomial theorem again, we find that

$$(3) \quad (a^r - b^r)/(a - b) = r\{b^{r-1} + \binom{r}{2} b^{r-2}h + \dots + r^{r-2}h^{r-1}\}.$$

Since  $r$  is prime,  $r$  divides  $\binom{r}{2} b^{r-2}h + \dots + r^{r-2}h^{r-1}$  unless  $r = 2$ . Since  $a - b$  and  $b$  are coprime,  $r$  does not divide  $b$ , so  $b^{r-1} \equiv 1 \pmod{r}$ , by Fermat's little theorem. Thus, by equation (3),  $(a^r - b^r)/(a - b) \equiv r \pmod{r^2}$  unless  $r = 2$ , whereas it follows from equation (2) that  $(a^r - b^r)/(a - b) \equiv 0 \pmod{r^2}$ . So  $r = 2$ ; equation (2) becomes  $a + b = 2^t$ , and it can be checked that  $a^2 - b^2$  does divide  $(a - b)^{t+1}$ .  $\square$

**THEOREM.** *If  $a$  and  $b$  are coprime and  $r$  is a natural number such that  $a^r - b^r$  divides a power of  $a - b$ , then  $r = 1$  or  $2$ . When  $r = 2$ ,  $a$  must be of the form  $2^t - b$ .*

*Proof.* If  $r = uv$  has a prime factor  $u \neq 2$  and  $a^r - b^r$  divides  $(a - b)^s$  for some  $s$ , then  $a^u - b^u$  divides  $(a - b)^s$ , contradicting the proposition above. So we may assume that  $r = 1$  or  $2^k$  for some  $k$ . Now,  $a + b$  divides  $(a^{2^k} - b^{2^k})/(a - b) = 2^{kt}$ , so  $a + b = 2^w$  for some  $w$ . Hence  $a^2 + b^2 = 2(2^{2w-1} + 2^w b + b^2)$ . Since  $a$  and  $b$  are coprime and  $a + b$  is even,  $b$  is odd, so  $2^{2w-1} + 2^w b + b^2$  is odd. But, if  $k > 1$ , then  $a^2 + b^2$  divides  $(a^{2^k} - b^{2^k})/(a - b) = 2^{kt}$ , a contradiction. So  $k = 1$ , and so  $r = 1$  or  $2$ . The case  $r = 1$  is trivial, and if  $r = 2$ , the theorem follows from the proposition above.  $\square$

*Remarks.* The question answered by the above theorem arose in [2], where it is shown that the natural split extension of the multiplicative group of  $\text{GF}[p^r]$ , ( $r > 1$ ), by the Galois group of  $\text{GF}[p^r]$  over  $\text{GF}[p]$ , is nilpotent precisely when  $p^r - 1$  divides a power of  $p - 1$ . If we set  $a = p$  and  $b = 1$ , then the proposition above tells us that  $p^r - 1$  divides a power of  $p - 1$  precisely when  $r = 2$  and  $p$  is a Mersenne prime.

The author would like to thank the referee for pointing out that the result just described can be generalized to the case of arbitrary coprime numbers  $a$  and  $b$ , and that these results can also be deduced from Theorem V of [1], which is proved by a different method.

#### REFERENCES

- [1] Geo. D. Birkhoff and H. S. Vandiver, *On the integral divisors of  $a^n - b^n$* , Ann. of Math. 5 (1904), 173-180.
- [2] W. H. Wilson, *Primitive Irreducible Linear Groups*, M.Sc. thesis, Australian National University, 1972.

University of Queensland  
St. Lucia, Brisbane 4067  
Australia

*Received June 22, 1977; revised July 29, 1977.*

