INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A20

ON MOD p LOGARITHMS $\log_a b$ AND $\log_b a$

Marcin Mazur
Department of Mathematics, Binghamton University, P.O. Box 6000, Binghamton, NY 13892-6000, USA
mazur@math.binghamton.edu

Received: 5/18/06, Accepted: 6/23/06, Published: 8/25/06

In 1997 A. Schinzel proposed the following problem.

Problem. Show that there is no constant c such that the equivalence

$$2^n \equiv 3 \pmod{p} \iff 3^n \equiv 2 \pmod{p}$$

holds for all prime numbers $p > c$ and all positive integers n.

Schinzel's problem was solved by G. Banaszak [1], who showed that there are infinitely many prime numbers p such that $2^n \equiv 3 \pmod{p}$ and $3^n \not\equiv 2 \pmod{p}$ for some integer n, and also there are infinitely many prime numbers p such that $2^n \not\equiv 3 \pmod{p}$ and $3^n \equiv 2 \pmod{p}$ for some n.

In this short note we prove two general results which imply analogous statements for many pairs of integers a, b instead of the pair $2, 3$.

For a positive integer a and a set P of prime numbers we define the P-part of a to be the unique divisor d of a such that all prime divisors of d belong to P and no prime divisor of a/d belongs to P.

Theorem 1. *Let $a > 1$, $b > 1$ be distinct integers. Define d to be the D-part of b, where D is the set of prime divisors of $\gcd(a, b)$. Let e be the P-part of $b - 1$, where P is the set of those prime divisors of $b - 1$ which do not divide a. Suppose that $a^2 \neq b + ed$. Then there are infinitely many primes p such that*

$$a^n \equiv b \pmod{p} \quad \textit{and} \quad b^n \not\equiv a \pmod{p}$$

for some positive integer n.

Proof. Let S be a finite set of prime numbers disjoint from D and containing all prime divisors of $ab-1$ and all prime divisors of $b-1$ which do not divide a. Suppose that S has the property that if q is a prime not in S and $q|(a^n-b)$ for some n then $q|(b^n-a)$. Set $m = e\prod_{q\in S}(q-1)$. By the Dirichlet's theorem on primes in arithmetic progression, there exist infinitely many primes p such that $m|p+1$. Choose any such prime p which is sufficiently large ($p > a^2+b+ed$ suffices). Then $d|(a^{p+1}-b)$ and no prime in D divides $(a^{p+1}-b)/d$. Also if q^t is the highest power of a prime q such that $q^t|e$ and $t>0$ then $(q-1)q^t|(p+1)$ and therefore $q^{t+1}|(a^{p+1}-1)$. It follows that $q^t|(a^{p+1}-b)$ and $q^{t+1}\nmid(a^{p+1}-b)$. Thus $e|(a^{p+1}-b)$ and no prime divisor of e divides $(a^{p+1}-b)/e$. Since $\gcd(e,d)=1$, we have $(a^{p+1}-b)/de$ is an integer.

Let q be a prime divisor of $(a^{p+1}-b)/ed$. Then

1. $\underline{q\nmid ab}$. This is clear, since $q\notin D$.
2. $\underline{q\notin S}$. Indeed, if $q\in S$ then $q-1|p+1$ and therefore $q|a^{p+1}-1$. Thus $q|(b-1)$ and therefore $q|e$. But no prime divisor if e divides $(a^{p+1}-b)/de$.
3. $\underline{q|(b^{p+1}-a)}$. This follows from our assumption about S and (2).
4. $\underline{q|(ab)^p-1}$. Indeed, multiplying the congruences

$$a^{p+1}\equiv b \pmod q\ , \quad b^{p+1}\equiv a \pmod q$$

   we get $(ab)^{p+1}\equiv ab \pmod q$ and our claim follows now from (1).
5. $\underline{q\equiv 1 \pmod p}$. Indeed let s be the order of ab modulo q. Then $s|q-1$ and $s|p$. If $s=1$ then $q|(ab-1)$ so $q\in S$, a contradiction. Thus $s>1$ and therefore $s=p$.

We proved that all prime divisors of $(a^{p+1}-b)/ed$ are congruent to 1 modulo p. Thus $(a^{p+1}-b)/ed\equiv 1 \pmod p$, i.e. $(a^{p+1}-b)\equiv ed \pmod p$. On the other hand, $(a^{p+1}-b)\equiv a^2-b \pmod p$, so $a^2\equiv b+ed \pmod p$. Since both a^2 and ed are smaller than p we have $a^2=b+ed$, a contradiction. This shows that a set S satisfying our assumptions cannot exist, i.e. Theorem 1 holds. □.

Example. If $a=3$ and $b=2$ then $d=1=e$ and $a^2=9\neq 3=b+ed$. Thus our theorem can be applied in this case. However, if $a=2$, $b=3$ then $e=1=d$ and $a^2=4=b+ed$ so Theorem 1 cannot be applied.

We need a slightly different approach in order to extend Theorem 1 to the case $a=2$, $b=3$. We keep the notation set in the statement of Theorem 1.

Theorem 2. *Let $r\nmid e$ be a fixed prime number. Suppose that there is a power $m=r^i$ of r such that $a^{m+1}-b$ has a prime divisor q_0 prime to b such that the order of b modulo q_0 is not a power of r. Then there are infinitely many primes p such that*

$$a^n\equiv b \pmod p \quad \text{and} \quad b^n\not\equiv a \pmod p$$

for some positive integer n.

Proof. Let S be a finite set of prime numbers disjoint from D and containing all prime divisors of $(ab)^m - 1$ and all prime divisors of $b-1$ which do not divide a. Suppose that S has the property that if q is a prime not in S and $q|(a^n - b)$ for some n then $q|(b^n - a)$. Fix a positive integer N such that r^N does not divide any of the numbers $q-1$ with $q \in S$ (so the r-part of $q-1$ divides r^N). For a prime divisor q of $(b^{r^N} - 1)$ which does not divide a define $q^{e(q)}$ as the highest power of q dividing $(b^{r^N} - 1)$ (note that $q \neq r$). There are infinitely many primes p such that $mp + 1$ is divisible by the following integers:

1. $q^{e(q)}$ for every prime divisor q of $(b^{r^N} - 1)$ which does not divide a;
2. the prime to r part of $q-1$ for every prime $q \in S$.

Choose any such prime p which is sufficiently large ($p > a^{m+1} + db^{r^N}$ suffices). Suppose that $q \in S$ and $q^f | a^{mp+1} - b$ for some $f > 0$. By our choice of p and N we have $(q-1)|r^N(mp+1)$ and $q \nmid a$. Thus $q|a^{r^N(mp+1)}-1$. It follows that $q|(b^{r^N}-1)$. By (1) we have $q^{e(q)}|(mp+1)$, which implies that $(q-1)q^{e(q)}|r^N(mp+1)$ and $q^{e(q)+1}|a^{r^N(mp+1)} - 1$. We conclude that $f \leq e(q)$. Indeed, otherwise we would have $q^{e(q)+1}|a^{mp+1} - b|a^{r^N(mp+1)} - b^{r^N}$, hence $q^{e(q)+1}|(b^{r^N} - 1)$ contrary to the definition of $e(q)$. Consequently, the S-part A of $a^{mp+1} - b$ divides $(b^{r^N} - 1)$. Now, as in the proof of Theorem 1, if q is a prime divisor of $(a^{mp+1} - b)/d$ which is not in S then $q|(ab)^{mp} - 1$. Since $q \notin S$, $(ab)^m - 1$ is not divisible by q. In other words, the order of ab modulo q divides mp but not m. It follows that this order must be divisible by p so $p|q-1$. This proves that $(a^{mp+1} - b)/dA \equiv 1 \pmod{p}$, i.e. $(a^{mp+1} - b) \equiv dA \pmod{p}$. On the other hand, $(a^{mp+1} - b) \equiv a^{m+1} - b \pmod{p}$. Since p is large, we conclude that $a^{m+1} - b = dA$. It follows that $q_0|A$, which contradicts our choice of q_0 (recall that $A|(b^{r^N} - 1)$). This shows that the set S does not exist and Theorem 2 holds. □

Example. If $a = 2$ and $b = 3$ we may take $r = 2$. Let $i = 2$ so $a^{m+1} - b = 29 = q_0$. The order of 3 modulo 29 is not a power of 2. In fact $28 = 4 \cdot 7$ and $3^4 - 1$ is not divisible by 29. So our theorem applies.

It seems plausible that the assumptions of Theorem 2 are always satisfied for some choice of a prime r, but we do not have a proof of this statement.

References

[1] G. Banaszak, *Mod p logarithms* $\log_2 3$ *and* $\log_3 2$ *differ for infinitely many primes,* Ann. Math. Silesianae 12 (1998), 141-148.