Annales Mathematicae Silesianae 12 (1998), 141–148

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

MOD p LOGARITHMS $\log_2 3$ AND $\log_3 2$ DIFFER FOR INFINITELY MANY PRIMES

GRZEGORZ BANASZAK

At the Thirteen Czech-Slovak International Number Theory Conference in Ostravice in 1997 and at JA in Limoges in 1997 A. Schinzel proposed the following problem.

PROBLEM 1. *Disprove the following statement.*

There exists such a prime number p_0, *that for all prime numbers* $p > p_0$ *and all* $n \in \mathbb{N}$ *the following condition holds*

$$2^n \equiv 3 \mod p \quad \Leftrightarrow \quad 3^n \equiv 2 \mod p.$$

We can reformulate Problem 1 in the following way.

Prove that for every prime number p_0 *there is a prime number* $p > p_0$ *and there is an* $n \in \mathbb{N}$ *such that either*

$$2^n \equiv 3 \mod p \quad \text{and} \quad 3^n \not\equiv 2 \mod p$$

or

$$2^n \not\equiv 3 \mod p \quad \text{and} \quad 3^n \equiv 2 \mod p.$$

We solve Problem 1 by proving the following theorem.

Received on September 28, 1998.

1991 *Mathematics Subject Classification..*

THEOREM 1.
(a) *For every prime number p_0 there is a prime number $p > p_0$ and there is an $n \in \mathbb{N}$ such that*

$$2^n \equiv 3 \; mod \; p \quad and \quad 3^n \not\equiv 2 \; mod \; p.$$

(b) *For every prime number p_0 there is a prime number $p > p_0$ and there is an $n \in \mathbb{N}$ such that*

$$3^n \equiv 2 \; mod \; p \quad and \quad 2^n \not\equiv 3 \; mod \; p.$$

PROOF. First we prove (a). The proof will be done in three steps.

Step 1. Let

$$p_1, p_2, p_3, \ldots$$

be the sequence of consecutive, odd prime numbers. Define a sequence of natural numbers

$$n_1 = p_1 - 1$$

$$n_2 = (p_1 - 1)(p_2 - 1)$$

$$\vdots$$

$$n_k = (p_1 - 1)(p_2 - 1) \ldots (p_k - 1)$$

$$\vdots$$

We observe that for each k

$$2^{n_k} - 3 \equiv -2 \; mod \; p_i$$

for all $1 \leqslant i \leqslant k$, by Little Fermat Theorem. It follows that $2^{n_k} - 3$ is divisible only by prime numbers bigger then p_k.

Step 2. Observe that for each $k > 1$ we have

$$2^{n_k} - 3 \equiv 5 \; mod \; 8$$

Numbers $1, 3, 5, 7$ are all odd residues *mod* 8. In addition

$$7^2 \equiv 1 \; mod \; 8$$

Hence for each k there must be a prime number p such that $p \equiv 3$ or $5 \mod 8$ and $2^{n_k} - 3 \equiv 0 \mod p$.

Step 3. Summing up, we proved in steps 1 and 2 the following fact.

For each $k > 1$ there is a prime number $p > p_k$ such that

(1) $2^{n_k} \equiv 3 \mod p$.
(2) $p \equiv 3$ *or* $5 \mod 8$

Observe that $3^{n_k} \not\equiv 2 \mod p$ because n_k is even. Indeed, we know that 2 is not a quadratic residue $\mod p$ for $p \equiv 3$ or $5 \mod 8$, cf. [H] p. 78.

Proof of (b) is based upon the idea of the proof of (a). Namely observe that:

(1) $3^{n_k} - 2 \equiv -2 \mod p_1$,
(2) $3^{n_k} - 2 \equiv -1 \mod p_i$ for $1 < i \leqslant k$,
(3) $3^{n_k} - 2 \equiv 7 \mod 12$ for $k \geqslant 1$.

Numbers $1, 5, 7, 11 \mod 12$ are all elements of the group $(\mathbb{Z}/12)^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$. Hence we get a prime number $p > p_k$ such that:

(4) $p \equiv 5$ or $7 \mod 12$,
(5) $3^{n_k} \equiv 2 \mod p$.

By quadratic reciprocity law [H] p. 79 we easily check that 3 is not a quadratic residue $\mod p$ iff $p \equiv 5$ or $7 \mod 12$. Hence $2^{n_k} \not\equiv 3 \mod p$ because n_k is even. $\square$

REMARK 1. Note that either part (a) or (b) of theorem 1 solve problem 1.

For p as in **Step 3** of (a) we prove that $3^n \not\equiv 2 \mod p$ for all n. Indeed, it follows by (1) in **Step 3** of (a) that 3 is a square $\mod p$ because n_k is even. Hence $\mod p$ logarithm $Log_3 2$ does not even exist for such a prime p.

In the same way for p from the proof of (b), we see that $\mod p$ logarithm $Log_2 3$ does not exist.

It is natural to ask for generalizations of Problem 1. Let us state the following problem suggested by A.Schinzel.

PROBLEM 2. *Let $a, b, c, d \in \mathbb{N}$ be such that $a > 1$, $c > 1$, $a \neq c$. Disprove the following statement.*
There exists such a prime number p_0, that for all prime numbers $p > p_0$ and all $n \in \mathbb{N}$ the following condition holds

$$a^n \equiv b \mod p \quad \Leftrightarrow \quad c^n \equiv d \mod p$$

REMARK 2. Problem 1 is a very special case of problem 2 with $a = d = 2$ and $b = c = 3$.

PROPOSITION 1.
(a) *For every prime number* p_0 *there is a prime number* $p > p_0$ *and there is an* $n \in \mathbb{N}$ *such that*

$$2^n \equiv 5 \; mod \; p \quad and \quad 5^n \not\equiv 2 \; mod \; p.$$

(b) *For every prime number* p_0 *there is a prime number* $p > p_0$ *and there is an* $n \in \mathbb{N}$ *such that*

$$5^n \equiv 2 \; mod \; p \quad and \quad 2^n \not\equiv 5 \; mod \; p.$$

PROOF. The proof is very similar to the proof of theorem 1. To prove (a) note that:

(1) $2^{n_k} - 5 \equiv -4 \; mod \; p_i$ for $1 \leqslant i \leqslant k$
(2) $2^{n_k} - 5 \equiv 3 \; mod \; 8$ for $k > 1$.

To prove (b) observe that

(1) $5^{n_k} - 2 \equiv -2 \; mod \; p_2$,
(2) $5^{n_k} - 2 \equiv -1 \; mod \; p_i$ for $i = 1$ or $2 < i \leqslant k$
(3) $5^{n_k} - 2 \equiv 3 \; mod \; 10$ for $k \geqslant 1$.

Numbers $1, 3, 7, 9 \; mod \; 10$ are all elements of the group $(\mathbb{Z}/10)^\times \cong \mathbb{Z}/4$. Note that $9^2 \equiv 1 \; mod \; 10$. So we get a prime number $p > p_k$ such that:

(4) $p \equiv 3$ or $7 \; mod \; 10$,
(5) $5^{n_k} \equiv 2 \; mod \; p$.

In addition 5 is not a quadratic residue $mod \; p$ iff $p \equiv 3$ or $7 \; mod \; 10$, by quadratic reciprocity law [H] p. 79. Hence $2^{n_k} \not\equiv 5 \; mod \; p$ because n_k is even. $\square$

REMARK 3. Proposition 1 shows that numbers $a = d = 2$ and $b = c = 5$ give another solution to Problem 2. We would like to point out, that the solution of Problem 2 in the case $b = d = 1$ and a, c arbitrary, follows from [CR-S] p. 277, theorem 1. The result of Corrales-Rodrigáñez and Schoof mentioned above is done over any number field and was further generalized by A. Schinzel [S].

THEOREM 2. *There are infinitely many tuples (a, b, c, d) giving solutions to the problem 2 with $b \neq 1$, $d \neq 1$.*

PROOF. The proof is based upon ideas of proofs of theorem 1 and proposition 1. Following notation of theorem 1 we take $r \in \mathbb{N}$ to be a natural number such that the prime number $p_{r+1} \equiv 3$ or $5 \; mod \; 8$. Let $m_0 \in \mathbb{N}$ be odd and let $m_1, m_2, \ldots, m_r$ be arbitrary positive integers. Let us define:

(1) $a_r = 2^{m_0} p_1^{2m_1} p_2^{2m_2} \ldots p_r^{2m_r}$

(2) $b_r = p_{r+1}$.

Observe that the number $a_r^{n_k/n_r} - b_r$ is not divisible by primes $p \leqslant p_{r+1}$. On the other hand by Little Fermat theorem

$$a_r^{n_k/n_r} - b_r \equiv 1 - p_{r+1} \; mod \; p_i,$$

for $r+1 < i \leqslant k$. Hence $a_r^{n_k/n_r} - b_r$ is only divisible by primes $p > p_k$. In addition

$$a_r^{n_k/n_r} - b_r \equiv 3 \;\; or \;\; 5 \; mod \; 8.$$

So, arguing in the same way as in the proof of theorem 1, we see that there is a prime number $p > p_k$ and $p \equiv 3$ or $5 \; mod \; 8$ such that

$$a_r^{n_k/n_r} - b_r \equiv 0 \; mod \; p.$$

On the other hand

$$b_r^{n_k/n_r} - a_r \not\equiv 0 \; mod \; p,$$

since 2 - hence also a_r - is not a square mod p. It follows that for each r as above we can take $a = d = a_r$ and $b = c = b_r$ to get a solution to problem 2. $\square$

We may consider a generalization of problem 2 into the setting of group schemes. Let $A/\mathbb{Q}$ be an abelian group scheme over $\mathbb{Q}$ (we understand under this notion a group scheme [B] whose group structure is abelian without further restrictions, cf. [Mi] for narrower definition), with some reasonably good model $\mathcal{A}/\mathbb{Z}$. It is natural to propose the following problem.

PROBLEM 3. *Let $x, y, w, z \in A(\mathbb{Q})$ be four points in the Mordell-Weil group $A(\mathbb{Q})$. Assume that x and w are non-torsion and $x \neq w$. Find additional conditions on x, y, w, z such that the following statement holds.*

There exists such a prime number p_0, that for all prime numbers $p > p_0$ and all $n \in \mathbb{N}$ the following condition holds

$$nx_p = y_p \;\; in \;\; \mathcal{A}_p(\mathbb{F}_p) \quad \Leftrightarrow \quad nw_p = z_p \;\; in \;\; \mathcal{A}_p(\mathbb{F}_p),$$

where $\mathcal{A}_p$ is the reduction of $\mathcal{A}$ mod p and points $x_p, y_p, w_p, z_p \in \mathcal{A}_p$ are reductions of x, y, w, z mod p respectively.

REMARK 4. Problem 3 is solved in the case when A is an elliptic curve and $y = z = 0$ [CR-S] p. 277, theorem 2. Actually the authors in [CR-S] deal with elliptic curves over any number field F. We have decided to formulate problem 3 for abelian schemes over $\mathbb{Q}$, however the reader can easily formulate appropriate problem over any number field.

REMARK 5. Problem 2 is a special case of problem 3. Problem 2 concerns the group scheme $\mathbb{G}_m/\mathbb{Q}$. Obviously, other interesting examples for A in problem 3 are those of elliptic curves and more generally, abelian varieties over $\mathbb{Q}$. Note that

$$\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times = \bigoplus_p \mathbb{Z} \oplus \{1, -1\}.$$

Hence $\mathbb{G}_m(\mathbb{Q})$ is not finitely generated and has infinite rank over $\mathbb{Z}$. On the other hand if A is an abelian variety [Mi] over $\mathbb{Q}$ then $A(\mathbb{Q})$ is a finitely generated abelian group by Mordell-Weil theorem. The $\mathbb{Z}$-rank of the Mordell-Weil group $A(\mathbb{Q})$ for abelian variety $A/\mathbb{Q}$ is very hard to compute and should equal (due to the conjecture of Birch-Swinnerton Dyer) the order of vanishing at $s = 1$ of Hasse-Weil zeta function of A.

REMARK 6. Problem 3 would have had some trivial solutions if we had alowed x and w to be torsion points. Namely, if x is a torsion point, we can always take such a natural number $m \in \mathbb{N}$ that $m^2 x = x$. Define $y = mx$, so we obviously get $my = x$. This easily implies that orders of x and y are equal and for every $n \in \mathbb{N}$; $nx = y$ if and only if $ny = x$, already in $A(\mathbb{Q})$. Hence due to a result of Katz [K] p. 501, we observe that for all $p > 2$ and for all $n \in \mathbb{N}$; $nx_p = y_p$ if and only if $ny_p = x_p$ *in* $\mathcal{A}_p(\mathbb{F}_p)$.

PROPOSITION 2. *Let F be a number field and let A/F be an abelian variety over F. Let $\mathcal{A}/\mathcal{O}_F$ be the Neron model (see [BLR]) of A over $\mathcal{O}_F$. Let k_v denote the residue field for a finite prime ideal in $\mathcal{O}_F$, and let $\mathcal{A}_v$ be the reduction at v. Then the natural map*

$$A(F) \to \prod_v \mathcal{A}_v(k_v)$$

is an injection.

PROOF. We know that torsion subgroup of $A(F)$ imbeds into $\prod_v \mathcal{A}_v(k_v)$ by a theorem of Katz [K] p. 501. We need to prove that non-torsion elements are not in the kernel of the map from the proposition. Take a projective imbedding $A/F \to \mathbb{P}^n/F$ such that the identity element of the abelian group $A(F)$ has projective coordinates $[1, 0, 0, \ldots, 0]$. Let $x \in A(F)$ be non-torsion. Let $x = [t_0, t_1, \ldots, t_n]$ in $\mathbb{P}^n$. Take v such that all non-zero coordinates t_i are prime to v. Let $\bar{t}_i$ denote the reduction mod v of the coordinate t_i. If x reduces to indentity in $\mathcal{A}_v(k_v)$ then there is $\lambda \in F$ prime to v such that

$$[\bar{t}_0, \bar{t}_1, \ldots, \bar{t}_n] \equiv [\bar{\lambda}, 0, 0, \ldots, 0] \ mod \ v$$

This shows that $t_i = 0$ for $1 \leqslant i \leqslant n$. Hence

$$x = [t_0, 0, \ldots, 0] = [1, 0, \ldots, 0] \in A(F) \subset \mathbb{P}^n(F).$$

□

REMARK 7. We can trivially check that for any finite set S of prime ideals in $\mathcal{O}_F$ the map

$$\mathcal{O}_{F,S}^\times \to \prod_{v \notin S} k_v^\times$$

is an injection. Observe that in the case of $\mathbb{G}_m$ we have

$$\mathbb{G}_m(F) = F^\times \neq \mathcal{O}_{F,S}^\times = \mathbb{G}_{m,\mathcal{O}_{F,S}}(\mathcal{O}_{F,S}).$$

It differs from the case of an abelian variety A/F and its Neron model $\mathcal{A}/\mathcal{O}_F$. Namely, we have

$$A(F) = \mathcal{A}(\mathcal{O}_F) \qquad \text{[K] p. 501.}$$

REMARK 8. Proposition 2 and remark 7 show some similarity between $\mathcal{O}_{F,S}^\times$ and $A(F)$ with respect to the problem of reduction modulo various primes v. However we would like to point out that the structure of $k_v^\times$ is much better known then the structure of $\mathcal{A}_v(k_v)$ as v varies. The reader easily observes that knowledge of the structure of multiplicative groups of residue fields $\mathbb{F}_p$ was one of main keys to the solution of Problem 1. In that case we dealt with the map

$$\mathbb{G}_m(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]) = (\mathbb{Z}[\frac{1}{2}, \frac{1}{3}])^\times \to \prod_{p>3} \mathbb{F}_p^\times = \prod_{p>3} \mathbb{G}_m(\mathbb{F}_p)$$

$$x \to (x_p)$$

Because of the structures of $\mathcal{A}_v(k_v)$ and Mordell-Weil group $A(F)$, problem 3 may be a little bit harder then problem 2.

Acknowledgments. I would like to thank A. Schinzel for valuable comments regarding first draft of this paper and for bringing to my attention the paper [C-RS]. I thank the referee for suggesting part (b) of theorem 1 which led me to figure out part (b) of Proposition 1.

References

[B] B.E. *Воскресенский*, *Алгебраические Торы*, *Издателство Наука, Москва* (1977).

[BLR] S. Bosch, W. Lutkebohmer, M. Raynaud, *Néron Models A Series of Modern Surveys in Mathematics*, Springer–Verlag (1990).

[C-RS] C. Corralez-Rodrigáñez, R. Schoof, *Support problem and its elliptic analogue*, Journal of Number Theory, **64** (1997), 276–290.

[H] H. Hasse, *Number Theory*, Akademie-Verlag, Berlin (1979).

[K] N.M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math., **62** (1981), 481–502.

[Mi] J.S. Milne, *Abelian varieties*, Arithmetic Geometry G. Cornell, J.H. Silverman (eds.), Springer-Verlag (1986), 103–150.

[S] A. Schinzel, *О показательных сравненях*, Математические Записки, **2** (1996), 121–126.

Department of Mathematics and Computer Sci.
Adam Mickiewicz University
Poznań
Poland

e-mail:
BANASZAK@math.amu.edu.pl