

## Sketch for Theorem 6 with $a$ composite

revised 13 Dec 2007

Reese Scott

Robert Styer (correspondence author), Dept. of Mathematical Sciences, Villanova University, 800 Lancaster Avenue, Villanova, PA 19085–1699, phone 610–519–4845, fax 610–519–6928, robert.styer@villanova.edu

Before proceeding we will need a few preliminaries. Suppose we have, for odd  $a > 1$  with  $a$  not necessarily prime,

$$\pm a^{x_1} \pm b^{y_1} = \pm a^{x_2} \pm b^{y_2} = c > 0, 1 \leq x_1 \leq x_2, 1 \leq y_1 \leq y_2, \quad (2)$$

where the  $\pm$  signs are independent and  $(x_1, y_1) \neq (x_2, y_2)$ . Clearly (49) can be rewritten as one of the following four types:

$$\text{Type 1 : } a^{x_1}(a^{x_2-x_1} - 1) = b^{y_1}(b^{y_2-y_1} - 1) \quad (2a)$$

$$\text{Type 2 : } a^{x_1}(a^{x_2-x_1} - 1) = b^{y_1}(b^{y_2-y_1} + 1) \quad (2b)$$

$$\text{Type 3 : } a^{x_1}(a^{x_2-x_1} + 1) = b^{y_1}(b^{y_2-y_1} - 1) \quad (2c)$$

$$\text{Type 4 : } a^{x_1}(a^{x_2-x_1} + 1) = b^{y_1}(b^{y_2-y_1} + 1) \quad (2d)$$

**Lemma 3** Let  $a > 1$  and  $b > 1$  be relatively prime integers. For  $1 \leq i \leq t$ , let  $p_i$  be one of the  $t$  distinct prime divisors of  $a$ . Let  $p_i^{g_i} \parallel b^{n_i} \pm 1$ , where  $n_i$  is the least number such that  $p_i | b^{n_i} \pm 1$  (when  $p_i = 2$  we choose the sign to maximize  $g_i$ ).

Write

$$S = \sum_i g_i \log(p_i) / \log(a).$$

Then, if

$$a^x | b^y \pm 1, \quad (17)$$

where the  $\pm$  sign is independent of the above, we must have

$$a^{x-S} | y.$$

Proof: Let  $a = \prod_i p_i^{\alpha_i}$ . If (17) holds, then for each  $i$ ,  $p_i^{x\alpha_i} | b^y \pm 1$ , so that  $p_i^{x\alpha_i - g_i} | y$  (in the case  $x\alpha_i < g_i$ ,  $p_i^{x\alpha_i - g_i}$  is a fraction that evenly divides  $y$ ). Thus,  $y$  is divisible by

$$\prod_i p_i^{x\alpha_i - g_i} = a^{x-S}.$$

**Lemma 4** If  $a > 2$  and  $(a, b) \neq (3, 2)$ , then, in the notation of Lemma 3,

$$S < \frac{a \log b}{2 \log a}.$$

Proof: We assume  $a > 2$  and  $(a, b) \neq (3, 2)$ . Then if  $a$  is odd,  $\prod_i p_i^{g_i} \leq b^{\phi(a)/2} + 1 \leq b^{(a-1)/2} + 1 < b^{a/2}$ , verifying Lemma 4 when  $a$  is odd. If  $a > 4$  is even, then  $\prod_i p_i^{g_i} \leq b^{\phi(a/2)} < b^{a/2}$  verifying the lemma in this

case also. Finally, when  $a = 4$ , define  $g$  so that  $2^g || b \pm 1$ , where the sign is chosen to maximize  $g$ . Then the lemma holds unless  $\frac{g \log(2)}{\log(4)} \geq \frac{4 \log(b)}{2 \log(4)}$ , that is, unless  $2^g \geq b^2$ , which is impossible.

**Lemma 5** Let  $a > 2$ ,  $b > 1$ , and  $c > 0$  be relatively prime integers. If (1) has two solutions  $(x_1, y_1)$  and  $(x_2, y_2)$ , with  $x_1 \leq x_2$  and  $y_1 \leq y_2$ , and if further  $a^{x_1} > c/2$ , then

$$x_1 < S + k,$$

where  $S$  is defined as in Lemma 3, and  $k = \frac{\log 3294.5 + \log \log a}{\log a}$  when  $a < 5346$  and  $k = 1.19407$  otherwise.

Proof: When  $(a, b) = (3, 2)$ , all cases in which (1) has more than one solution are given in [Pi] and the Corollary to Theorem 2 of [Sc-St]; the lemma holds in all these cases, so we assume from here on that  $(a, b) \neq (3, 2)$ .

If  $y_1 = y_2$ , then, using (6) with the roles of  $a$  and  $b$  reversed, we see that  $x_1 = 1$ ; so we can take  $y_1 < y_2$ . Following closely the method of proof in Bennett's Proposition 4.4 [Be], assume there are two solutions to (1) with  $a^{x_1} > c/2$ ,  $y_2 > y_1$ , and  $x_2 \geq x_1 = S + k_1$  with  $k_1 \geq k$ , where  $k$  is defined for each  $a$  as in the formulation of this lemma. From the equation

$$a^{x_1}(a^{x_2-x_1} \pm 1) = b^{y_1}(b^{y_2-y_1} \pm 1)$$

it follows that

$$b^{y_2-y_1} \equiv \pm 1 \pmod{a^{x_1}}$$

and so Lemma 3 implies that  $y_2 - y_1 \geq a^{x_1-S}$ . Thus,

$$y_2 > a^{k_1}.$$

On the other hand,  $c < 2a^{x_1}$ , so

$$\log c < x_1 \log a + \log 2 = (S + k_1) \log a + \log 2.$$

So now we have

$$\frac{y_2 \log b}{\log c} > \frac{a^{k_1} \log b}{(S + k_1) \log a + \log 2}.$$

From Lemma 4 we have

$$S < \frac{a \log b}{2 \log a}$$

and so

$$\frac{y_2 \log b}{\log c} > \frac{a^{k_1}}{\left(\frac{a}{2 \log a} + \frac{k_1}{\log b}\right) \log a + \frac{\log 2}{\log b}} > 10.519$$

where the second inequality follows from  $k_1 \geq k$ ,  $a \geq 3$ , and  $b \geq 2$ . Let

$$G = \max \left\{ \frac{x_2}{\log b}, \frac{y_2}{\log a} \right\}.$$

Then we have

$$\frac{G}{5.2595} \geq \frac{y_2}{5.2595 \log a} > \frac{2 \log c}{\log a \log b} \tag{19}.$$

Now let  $\Lambda = |x_2 \log a - y_2 \log b|$ . Applying a theorem of Mignotte as given in Section 3 of [Be], and using in Mignotte's formula the parameters chosen by Bennett in the proof of Proposition 4.4 of [Be], we see that we must have either

$$G < 3294.5 \tag{20}$$

or

$$\log \Lambda > -24.2(\log G + 2.4)^2 \log a \log b. \tag{21}$$

First assume  $c > 1$ . Assume (21) holds. Then, in the same way we derived (11) in the proof of Theorem 2 (here  $c_1 = c$ ), we obtain

$$G < 2 \frac{\log c}{\log a \log b} + 24.2(\log G + 2.4)^2. \tag{22}$$

Using (19) we obtain

$$G < 29.882(\log G + 2.4)^2,$$

which implies  $G < 3294.5$ . So, no matter which of (20) or (21) holds, we have

$$3294.5 > G \geq \frac{y_2}{\log a} > \frac{a^{k_1}}{\log a},$$

which is impossible since  $k_1 \geq k$ .

Now assume  $c = 1$ , so that  $\Lambda < \log 2$ . Proceeding as with  $c > 1$ , it is easily seen we can replace (22) by

$$G < \frac{\log 2}{\log a \log b} + 24.2(\log G + 2.4)^2. \tag{23}$$

From (23) we again derive

$$\frac{a^{k_1}}{\log a} < 3294.5,$$

impossible since  $k_1 \geq k$ .

The following generalizes Observation 8 of [Sc-St2] to include composite values of  $a$ .

**Lemma 5** : If  $M > 3$  is a Mersenne number with  $M = 2^u - 1$ , then the only solutions to (2) with  $a = M$  are

$$M + 2 = 2^{u+1} - M = c_1, \tag{6a}$$

$$M + 2^u = 2^{2u} - M^2 = c_2. \tag{6b}$$

If  $F > 5$  is a Fermat number with  $F = 2^v + 1$ , then the only solutions to (2) with  $a = F$  are

$$F - 2 = 2^{v+1} - F = c_3, \tag{6c}$$

$$F + 2^v = F^2 - 2^{2v} = c_4. \tag{6d}$$

Proof of Lemma 5: In what follows we refer to a solution to (2) with  $b = 2$ . It is easy to see that, for  $b = 2$ , (2a), (2b), (2c), and (2d) require  $y_1 < y_2$ .

By Lemma 4,  $x_1 = 1$ .

If (2a) has a solution with  $a = 2^n \pm 1$  with  $x_2$  odd, then we must have  $y_1 > n$ ; but, by Theorem 4 of [Sc-St],  $2^{y_1} < a^{x_1} = a$ , contradiction. If (2a) has a solution with  $a = 2^n + 1$  and  $x_2$  even, we have  $y_1 = n$ , so that  $c = 1$  in (2), which is impossible for  $a > 3$ . If (2a) has a solution with  $a = 2^n - 1$  and  $x_2$  even, we have  $y_1 = 1$ ,  $a^{x_2} - a^{x_1} \equiv 6 \pmod{8}$ ,  $2 \mid x_1 = 1$ , contradiction. Thus, there are no Type I solutions to (2) when  $a = 2^n \pm 1$ .

By Observation 2 of [Sc-St2], (2b) has no solutions with  $a = 2^n - 1$ . If (2b) has a solution with  $a = 2^n + 1$  and  $x_2$  odd, then  $(a + 1)/2 = 2^{n-1} + 1$  divides both sides of (2b), so that  $y_2 - y_1$  must be an odd multiple of  $n - 1$ ; but  $a$  also divides both sides of (2b), so that  $y_2 - y_1$  must be an odd multiple of  $n$ , contradiction. If (2b) has a solution with  $a = 2^n + 1$  and  $x_2$  even, then  $y_1 = n$ , so that  $c = c_4$ ; by Theorem 1 of [Sc-St2], the only possible case is given by (6d).

By Observation 3 of [Sc-St2], (2c) has no solutions with  $a = 2^n + 1$ . If (2c) has a solution with  $a = 2^n - 1$  then we must have either  $y_1 = 1$  or  $y_1 = n$  according as  $x_2$  is either odd or even, so that  $c = c_1$  or  $c_2$ ; but by Theorem 1 of [Sc-St2] the only possible cases are given by (6a) and (6b).

By Observation 2 of [Sc-St2], (2d) has no solutions with  $a = 2^n - 1$ . Any solutions with  $a^n + 1$  must have  $y_1 = 1$ , so that  $c = c_3$ ; by Theorem 1 of [Sc-St2], the only case is given by (6c). This completes the proof of Lemma 5.