Non-congruent Numbers with Arbitrarily Many Prime Factors Congruent to 3 Modulo 8

By Boris ISKRA

Department of Mathematics, University of Illinois, U.S.A.

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1996)

Introduction. In this paper we are going to show the existence of an infinite set of primes congruent to 3 modulo 8, such that any product of primes in this set is a non-congruent number. The existence of such a sequence implies the existence of an elementary 2-extension of infinite degree over which the rank of the elliptic curve $E : y^2 = x^3 - x$ remains zero. The question about the existence of such an extension was posed by Kida in [1] §3. The proof below is based on a result of Serf [2] which gives an upper bound for the rank of the elliptic curve $E_n : y^2 = x^3 - n^2x$.

Theorem. *Let $p_1, \ldots, p_l$ be distinct primes such that $p_i \equiv 3 \pmod 8$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_l$ is a non-congruent number.*

Notes:

1) Since $p_i \equiv 3 \pmod 8$,
$$\left(\frac{-1}{p_i}\right) = \left(\frac{2}{p_i}\right) = -1.$$

2) $$\left(\frac{p_j}{p_i}\right) = 1 \text{ if } i < j.$$

3) Let $n = n_i \cdot p_i$; then
$$\left(\frac{n_i}{p_i}\right) = (-1)^{i-1}.$$

4) Let b be a divisor of n, and put
$$b' = \frac{b}{p_i} \text{ if } p_i \mid b,$$
$$= b \text{ if } p_i \nmid b.$$
Let $k = |\{j : p_j \mid b \text{ and } j < i\}|$; then
$$\left(\frac{b'}{p_i}\right) = (-1)^k.$$

Proof. To show that n is a non-congruent number we will use Theorem 3.3 and Corollary 3.4 in [2] to see that for all pairs $(b_1, b_2) \notin \{(1,1); (-1, -n); (n, 2); (-n, -2n)\}$ with $b_i \in \{\pm 2^{\varepsilon} p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l} \mid \varepsilon, \varepsilon_1, \ldots, \varepsilon_l \in \{0,1\}\}$ there is no solution for the system of equations:
$$\left\{\begin{array}{l} b_1 z_1^2 - b_2 z_2^2 = n \\ b_1 z_1^2 - b_1 b_2 z_3^2 = -n \end{array}\right\}$$

Using the general unsolvability-condition and the unsolvability-condition mod 2 in [2] §3, we are left with $b_1 \cdot b_2 > 0$ and $2 \nmid b_1$.

Case 1. $b_2 > 0$ and $2 \nmid b_2$. Define
$$r = min\{i \,; p_i \mid b_1 \text{ or } p_i \mid b_2\}$$
If r exists then
$$\left(\frac{b_1'}{p_r}\right) = 1$$
$$\left(\frac{b_2'}{p_r}\right) = 1$$
If $p_r \mid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,1)$ and
$$\left(\frac{-n_r b_1'}{p_r}\right) = -(-1)^{r-1} = (-1)^r$$
$$\left(\frac{-2n_r b_2'}{p_r}\right) = (-1)^{r-1}$$
One of the two Jacobi symbols is equal to -1 and therefore there is no solution.

If $p_r \mid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,0)$ and
$$\left(\frac{2b_2}{p_r}\right) = -1$$
and there is no solution.

If $p_r \nmid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,1)$ and
$$\left(\frac{-b_1}{p_r}\right) = -1$$
and there is no solution.

Therefore r does not exist, which implies that no prime divides b_1 or b_2 and then $(b_1, b_2) = (1,1)$.

Case 2. $b_2 > 0$ and $2 \mid b_2$.

Define
$$r = min\{i : p_i \nmid b_1 \text{ or } p_i \mid b_2\}$$
If r exists then
$$\left(\frac{b_1'}{p_r}\right) = (-1)^{r-1}$$
$$\left(\frac{b_2'}{p_r}\right) = -1$$
If $p_r \nmid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,1)$ and

$$\left(\frac{-b_1}{p_r}\right) = -(-1)^{r-1} = (-1)^r$$
$$\left(\frac{-n_r b_2'}{p_r}\right) = -(-1)^{r-1}(-1) = (-1)^{r-1}$$

One of the two Jacobi symbols is equal to -1 and therefore there is no solution.

If $p_r \mid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,1)$ and

$$\left(\frac{-n_r b_1'}{p_r}\right) = -(-1)^{r-1}(-1)^{r-1} = -1$$

and there is no solution.

If $p_r \nmid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,0)$ and

$$\left(\frac{b_2}{p_r}\right) = -1$$

and there is no solution.

Therefore r does not exist, which implies that all the primes divide b_1 and no prime divides b_2, so $(b_1, b_2) = (n, 2)$.

Case 3. $b_2 < 0$ and $2 \nmid b_2$.

Define

$$r = min\{i : p_i \mid b_1 \text{ or } p_i \nmid b_2\}$$

If r exists then

$$\left(\frac{b_1'}{p_r}\right) = -1$$
$$\left(\frac{b_2'}{p_r}\right) = -(-1)^{r-1} = (-1)^r$$

If $p_r \mid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,0)$ and

$$\left(\frac{n_r b_1'}{p_r}\right) = (-1)^{r-1}(-1) = (-1)^r$$
$$\left(\frac{2b_2}{p_r}\right) = -(-1)^r = (-1)^{r-1}$$

One of the two Jacobi symbols is equal to -1 and therefore there is no solution.

If $p_r \mid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,1)$ and

$$\left(\frac{-2n_r b_2'}{p_r}\right) = (-1)^{r-1}(-1)^r = -1$$

and there is no solution.

If $p_r \nmid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,0)$ and

$$\left(\frac{b_1}{p_r}\right) = -1$$

and there is no solution.

Therefore r does not exist, which implies that no prime divide b_1 and all primes divides b_2, so $(b_1, b_2) = (-1, -n)$.

Case 4. $b_2 < 0$ and $2 \mid b_2$.

Define

$$r = min\{i : p_i \nmid b_1 \text{ or } p_i \nmid b_2\}$$

If r exists then

$$\left(\frac{b_1'}{p_r}\right) = -(-1)^{r-1} = (-1)^r$$
$$\left(\frac{b_2'}{p_r}\right) = (-1)^{r-1}$$

If $p_r \nmid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,0)$ and

$$\left(\frac{b_1}{p_r}\right) = (-1)^r$$
$$\left(\frac{b_2}{p_r}\right) = (-1)^{r-1}$$

One of the two Jacobi symbols is equal to -1 and therefore there is no solution.

If $p_r \nmid b_1$ and $p_r \mid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (0,1)$ and

$$\left(\frac{-n_r b_2'}{p_r}\right) = -(-1)^{r-1}(-1)^{r-1} = -1$$

and there is no solution.

If $p_r \mid b_1$ and $p_r \nmid b_2$ then $(v_{p_r}(b_1), v_{p_r}(b_2)) = (1,0)$ and

$$\left(\frac{n_r b_1'}{p_r}\right) = (-1)^{r-1}(-1)^r = -1$$

and there is no solution.

Therefore r does not exist, which implies that all primes divide b_1 and b_2 so $(b_1, b_2) = (-n, -2n)$.

Corollary 1. There exists an infinite sequence of distinct primes congruent to 3 modulo 8 such that any product of primes in this sequence is a non-congruent number.

Proof. It is enough to show that for every $l \in \boldsymbol{N}$ there exist $p_1, \ldots, p_l$, distinct primes $p_i \equiv 3 \pmod 8$, such that $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. This is clear by induction using Dirichlet's theorem on primes in arithmetic progression.

Acknowledgment. I would like to thank Prof. N. Boston for suggesting the problem to me and also for his valuable hints.

References

[1] M. Kida: On the rank of an elliptic curve in elementary 2-extensions. Proc. Japan Acad., **69A**, 422–425 (1993).

[2] P. Serf: Congruent Numbers and Elliptic Curves. Computational Number Theory. Walter de Gruyter and Co. Berlin, New York, pp. 227–238 (1991).