A Note on the 2-Part of Ш for the Congruent Number Curves

D.R. Heath-Brown
Mathematical Institute, Oxford

February 19, 2007

The purpose of this note is to give a brief exposition of the results of the author's work [1,2]. The congruent number problem is described by the quadratic twists of the elliptic curve

$$E : y^2 = x^3 - x,$$

that is to say, by the curves

$$E_D : Dy^2 = x^3 - x$$

for positive square-free integers D. The L-functions for these twists have even functional equation for $D \equiv 1, 2, 3 \pmod 8$, and odd functional equation for $D \equiv 5, 6, 7 \pmod 8$. The group Ш is described in Silverman [3; page 297]. In order to describe the 2-part of $Ш(D)$ it will be convenient to make the following hypothesis, which we shall assume throughout this note.

Hypothesis *There are $O(X(\log X)^{-2})$ positive square-free integers $D \leq X$ with $D \equiv 1, 2$ or $3 \pmod 8$ such that E_D has rank different from zero. Similarly there are $O(X(\log X)^{-2})$ positive square-free integers $D \leq X$ with $D \equiv 5, 6$ or $7 \pmod 8$ such that E_D has rank different from one.*

The order of the Selmer group $S^{(2)}$ is connected to the 2-part of Ш as follows. Let $\#S^{(2)} = 2^{2+s(D)}$, so that $s(D)$ is the upper bound for the rank of E_D which arises from the 2-descent process, see Silverman [3; page 281]. In the appendix to [2] Monsky showed that $s(D)$ is even for integers $D \equiv 1, 2, 3 \pmod 8$, and odd for values $D \equiv 5, 6, 7 \pmod 8$. Now define

$$Ш_2(D) = \{g \in Ш(D) : g \text{ has order 1 or 2}\}.$$

Then if $D \equiv 1, 2, 3 \pmod 8$ and E_D has rank zero, we have

$$\#Ш_2(D) = 2^{s(D)},$$

while if $D \equiv 5, 6, 7 \pmod 8$ and E_D has rank one, then

$$\#Ш_2(D) = 2^{s(D)-1}.$$

The main result of [1] gives the frequency with which each value of $s(D)$ occurs. Let

$$\lambda = \prod_{n=0}^{\infty}(1 - 2^{-2n-1}) = 0.4194\ldots$$

and set

$$d_k = \lambda \frac{2^k}{\prod_{1 \le j \le k}(2^k - 1)}, \quad (k = 0, 1, 2, \ldots).$$

Moreover we define

$$N(X; h) = \#\{D \le X : D \text{ square-free}, D \equiv h \pmod 8\},$$

$$N_s(X, k; h) = \#\{D \le X : D \text{ square-free}, s(D) = k, D \equiv h \pmod 8\}$$

and

$$N_{Ш}(X, k; h) = \#\{D \le X : D \text{ square-free}, \#Ш_2(D) = 2^{2k}, D \equiv h \pmod 8\}.$$

Theorem *If $h = 1$ or 3 then*

$$\frac{N_s(X, 2k; h)}{N(X; h)} \to d_{2k}, \quad (X \to \infty),$$

while if $h = 5$ or 7 then

$$\frac{N_s(X, 2k+1; h)}{N(X; h)} \to d_{2k+1}, \quad (X \to \infty).$$

Thus, under our hypothesis, it follows that if $h = 1$ or 3 then

$$\frac{N_{Ш}(X, k; h)}{N(X; h)} \to d_{2k}, \quad (X \to \infty),$$

while if $h = 5$ or 7 then

$$\frac{N_{Ш}(X, k; h)}{N(X; h)} \to d_{2k+1}, \quad (X \to \infty).$$

It is interesting to investigate the situation in which one restricts the number $\omega(D)$ of prime factors of D. When D is prime one finds that $s(D) = 2$ for every $D \equiv 1 \pmod 8$ and $s(D) = 0$ for every $D \equiv 3 \pmod 8$. When D is a product of two primes and $D \equiv 1 \pmod 8$ the cases $S(D) = 0, 2, 4$ occur with frequency $1/4, 5/8, 1/8$, while if $D \equiv 3 \pmod 8$ the cases $S(D) = 0, 2$ each occur with frequency $1/2$. As the number of prime factors grows these frequencies tend to the values $d_0, d_2, d_4, \ldots$, whether one restricts to $D \equiv 1 \pmod 8$ or to $D \equiv 3 \pmod 8$. Thus one sees firstly that, for $\omega(D)$ small, the proportions depend heavily on the congruence value of D modulo 8, and secondly that the proportions differ from their limiting values quite significantly. The following table illustrates this. The figures aggregate the cases in which $D \equiv 1 \pmod 8$ and $D \equiv 3 \pmod 8$, and also the cases in which $D \equiv 5 \pmod 8$ and $D \equiv 7 \pmod 8$.

	$k = 3$	$k = 5$	$k = 10$	$k = 20$	$k = \infty$
$s(D) = 0$	0.1875	0.1785	0.1905	0.2083	0.2097
$s(D) = 1$	0.3641	0.3650	0.4004	0.4163	0.4194
$s(D) = 2$	0.2607	0.2719	0.2883	0.2841	0.2796
$s(D) = 3$	0.1220	0.1239	0.0994	0.0784	0.0799
$s(D) = 4$	0.0531	0.0441	0.0174	0.0120	0.0107
$s(D) = 5$	0.0102	0.0135	0.0033	0.0009	0.0007
$s(D) = 6$	0.0024	0.0029	0.0006	0.0000	0.0000
$s(D) = 7$	0.0000	0.0002	0.0001	0.0000	0.0000

Table 1: Estimated Frequency of Selmer Ranks for $\omega(D) = k$

The table shows that when D has rather few prime factors the proportion of values $s(D) = 0, 1$ is less than in the limiting case. Even with $\omega(D) = 10$ the agreement is not very good. The reader should recall that for $D \leq 10^{10}$, say, one typically has $\omega(d)$ around 3. Thus one cannot expect the currently available numerical data to show good agreement with the theoretical limiting behaviour.

For the proof of the theorem, the starting point is the fact that the Selmer group $S^{(2)}$ has as elements those pairs

$$(a, b) \in \left(\frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \right)^2$$

for which the simultaneous equations

$$abx^2 + Dy^2 = az^2, \;\; abx^2 - Dy^2 = bw^2 \tag{1}$$

have non-trivial solutions in every completion of $\mathbb{Q}$. (There is a minor abuse of notation here, identifying $a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ with one of its coset representatives.) When D is odd one then finds, see [1], that $2^{s(D)}$ is given by the number of pairs for which a and b are positive divisors of D. Moreover the local conditions reduce to the requirement that the system (1) has solutions in $\mathbb{Q}_p$ for every prime divisor p of D. Finally, this last condition is satisfied if and only if the four equations

$$abx^2+Dy^2 = az^2, \;\; abx^2-Dy^2 = bw^2, \;\; 2abx^2 = az^2+bw^2, \;\; 2Dy^2 = az^2-bw^2$$

are individually solvable in $\mathbb{Q}_p$.

This analysis immediately shows that $s(D) \leq 2\omega(D)$. Moreover one can easily read off the frequency of the different values of $s(D)$ when D has at most two prime factors, say. The theorem given above however requires a computation of all the integer moments of $2^{s(D)}$, and this turns out to require a rather lengthy combinatorial argument.

References

[1] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem, *Invent. math.*, 111 (1993), 171-195.

[2] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem, II, *Invent. math.*, 118 (1994), 331-370.

[3] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, (Springer-Verlag, New York, 1992).