AN APPLICATION OF THE θ-CONGRUENT NUMBERS IN CRYPTOGRAPHY

T. Chantladze, N. Kandelaki, Z. Kipshidze, D. Ugulava

Georgian Technical University
Niko Muckhelishvili Institute of Computational Mathematics
0160 Akuri street 8, Tbilisi, Georgia

(Received: 23.07.13; accepted: 11.012.13)

Abstract

Points of infinity order for elliptic curves related to θ-congruent numbers are found. A cryptosystem created by reduction of such curves over finite fields is considered. An example illustrating the cryptosysrem is given.

Key words and phrases: θ-congruent numbers, elliptic curves, cryptography, finite fields, discrete logarithm.

AMS subject classification: 94A60, 14H52, 11T71.

It is shown in [1] how to construct open-key criptosystems by means of finite groups created by special subsets of finite fields. Consequently, given any such new group we are able to create a new criptosystem. For example, this problem can be solved by means of an elliptic curve over the field Q of rational numbers on which a point of infinite order is given [1]. In this paper we solve this problem by use of the so called θ-congruent numbers. The θ-congruent numbers represent the generalization of the congruent numbers that are well-known in the number theory. They were introduced and studied by M.Fujivara and his students [2]-[4]. For the sake of clearness we give the definition of a θ-congruent number and assertions that are of importance for us.

Let X, Y, Z are rational sides of a triangle and denote by θ the angle between X and Y. $\cos\theta$ is necessarily rational and we denote $\cos\theta = s/r$ $(r > 0,\ (r,s) = 1)$. Then $\sin\theta = \alpha_\theta/r$, where $\alpha_\theta = \sqrt{r^2 - s^2}$ is uniquely determined by θ. A square free natural number n is a θ-congruent number if there exists a triangle, whose sides are rational, one angle is θ and the area of triangles is $n\alpha_\theta$. A θ-congruent number n for $\theta = \pi/2$ is nothing but an ordinary congruent number, since $\alpha_{\pi/2} = 1$. In this case n coincides with the area of a rectangular triangle. The θ congruent numbers is full completely stated in the monograph [5] by N.Koblitz.

θ-congruent numbers are related with the equation of the elliptic curves

$$E_{n,\theta}:\ y^2 = x(x + (r+s)n)(x - (r-s)n). \tag{1}$$

Namely, in [2] it is proved that a number $n(\neq 1,2,3,6)$ is θ-congruent if and only if the elliptic curve $E_{n,\theta}$ has at least one nontrivial point (x,y), having infinite order (that is the rank of $E_{n,\theta}$ is non-zero). In this connection under the trivial points are implied the points $(0,0), (-(r+s)n, 0), ((r-s)n, 0)$ and the so-called infinite point of the curve $E_{n,\theta}$. Moreover, based on the well-known theorems of Nagell-Lutz and Mazur, it is proved in [6] that if a free from squares natural number n is not equal to 1,2,3 and 6, then the group of rational points of $E_{n,\theta}$ having $E_{n,\theta}$ finite order is isomorphic to the $Z_2 \oplus Z_2$, that is $\mathrm{tors\ E_{n,\theta}(Q)} = 4$.

First of all, in the sequel, we construct an infinite order rational point on $E_{n,\theta}$ with the help of θ-congruent number $n(\neq 1,2,3,6)$, corresponding to a triangle.

Let us consider a triangle whose sides are rational numbers X, Y, Z and the opposite angle of Z is θ. Let further $\cos\theta = s/r,\ \sin\theta = \alpha_\theta/r$. Instead of α_θ we will write simply α. Then

$$X^2 + Y^2 - 2XYs/r = Z^2.$$

Let us rewrite this equation in the form

$$\left(\frac{rX - sY}{rZ}\right)^2 + \frac{\alpha^2}{r^2}\left(\frac{Y}{Z}\right)^2 = 1.$$

Under the notations

$$u = \frac{rX - sY}{rZ},\ v = \frac{Y}{Z},$$

we obtain that $u^2 + \alpha^2 v^2/r^2 = 1$. This means that the point (u,v) lies on the ellipse whose semiaxes are 1 and r/α.Let $\alpha, 0 < \alpha < \pi/2$, be the angle between the segment connecting the points $(-1,0)$ and (u,v) and the positive direction of the axes u. Let $\tan\alpha = b/a$, where a and b are relatively prime natural numbers. Then

$$\begin{cases} v = (u+1)b/a, \\ u^2 + \alpha^2 v^2/r^2 = 1. \end{cases}$$

From here we obtain the quadratic equation

$$(a^2r^2 + r^2\alpha^2b^2)^2u^2 + 2\alpha^2b^2u + \alpha^2b^2 - r^2a^2 = 0$$

whose solutions are

$$u_1 = -1 \quad \text{and} \quad u_2 = \frac{r^2a^2 - \alpha^2b^2}{r^2a^2 + \alpha^2b^2}\ .$$

The corresponding values of v are

$$v_1 = 0 \quad \text{and} \quad v_2 = \frac{2abr^2}{r^2a^2 + \alpha^2 b^2} \ .$$

Since $v \neq 0$, we have

$$\frac{Y}{Z} = \frac{2abr^2}{a^2r^2 + \alpha^2 b^2} \quad , \quad \frac{X}{Z} = u + \frac{sY}{rZ} = \frac{a^2r^2 - \alpha^2b^2 + 2abrs}{a^2r^2 + \alpha^2 b^2} \ . \tag{2}$$

It follows from here that there exists a rational number l, for which

$$X = (a^2r^2 - (r^2 - s^2)b^2 + 2abrs)l,$$

$$Y = 2abr^2 l, \ Z = (a^2r^2 + (r^2 - s^2)^2 b^2)l \ . \tag{3}$$

If the area of the triangles whose sides are X, Y, Z is $n\alpha$, then

$$n = (a^2r^2 - (r^2 - s^2)b^2 + 2abrs)abrl^2 \ . \tag{4}$$

By means of representation (4) we can construct θ-congruent numbers. Namely, if a and b are any relatively prime natural and a rational number l is selected so that the right side of the last equality is a free of square natural number n, then it is θ-congruent. According to what has been said above, the number of finite order rational points is equal to 4 if θ-congruent number is selected so that $n \neq 1, 2, 3, 6$. To this end, for example, it is sufficient so select a and b that

$$(a, b) = 1, \ (a, r) = 1, \ (b, r) = 1, \ (a, r^2 - s^2) = 1 \ . \tag{5}$$

Finding such an n and based on formulas (3), we will have a triangle with rational sides X, Y, Z in which the opposite side of θ is Z. Now we can find nontrivial rational points of infinite order. Let us find a point (x, y) having this property in the following form

$$\begin{cases} x = -n\alpha^2 t/r, \\ y = \pm n^2\alpha^2(1 + \alpha^2t^2r^{-2})/Z \ . \end{cases} \tag{6}$$

After calculation of the right side of (1) by means of (6), we obtain

$$x(x + (r+s)n)(x - (r-s)n) = x(x^2 + 2snx - (r^2 - s^2)n^2)$$

$$= -\frac{n\alpha^2 t}{r}\left(\frac{n^2\alpha^4t^2}{r^2} - \frac{2sn^2\alpha^2t}{r} - \alpha^2n^2\right) = \frac{n^3\alpha^4 t}{r^3}(-\alpha^2t^2 + 2srt + r^2) \ .$$

For the calculation of y^2 we found that

$$\frac{n}{Z^2} = \frac{1}{2r} \cdot \frac{X}{Z} \cdot \frac{Y}{Z}.$$

Replacing the parameter t in (6) by the rational noncancellable number b/a, we obtain from (2) that

$$\frac{X}{Z} = \frac{r^2 - \alpha^2 t^2 + 2srt}{r^2 + \alpha^2 t^2}\ , \quad \frac{Y}{Z} = \frac{2r^2 t}{r^2 + \alpha^2 t^2}\ .$$

Therefore

$$\frac{n}{Z^2} = \frac{r^2 t(r^2 - \alpha^2 t^2 + 2srt)}{r(r^2 + \alpha^2 t^2)^2\ ,}$$

and

$$y^2 = \frac{n^4 \alpha^4}{Z^2} \cdot \frac{(r^2 + \alpha^2 t^2)^2}{r^4} = \frac{n^3 \alpha^4 t(r^2 - \alpha^2 t^2 + 2srt)}{r^3}\ .$$

Let us express the parameter t by means of the sides X, Y, Z. We have

$$\frac{X}{Z} - \frac{s}{r} \cdot \frac{Y}{Z} + 1 = \frac{2r^2}{r^2 + \alpha^2 t^2} = \frac{Y}{Z} \cdot \frac{1}{t}\ ,$$

and therefore

$$t = \frac{rY}{rX - sY + rZ}\ .$$

We have founded rational points $P(x, y)$ of infinite order lying on the curve (1) with the coordinates

$$x = -\frac{XY^2(r^2 - s^2)}{2r(rX - sY + rZ)}\ , \quad y = \pm\frac{X^2Y^2(r^2 - s^2)}{2r(rX - sY + rZ)}\ . \tag{7}$$

It is clear that $rX - sY + rZ > 0$ and therefore the abscissa of the obtaining points is negative.

Besides defining by (7) nontrivial points there exist yet lying on (1) two points, whose abscissa is $x = (Z/2)^2$ [2]. The second coordinates of these points are $y = \pm(X^2 - Y^2)Z/8$. The points (7) are important because they represent a nontrivial points of (1) for arbitrary sides X, Y, Z. In the case when the numbers a and b from (3) satisfy conditions (5), we obtain that $X \neq Y$ and the points $((Z/2)^2, \pm(X^2 - Y^2)Z/8)$ would have infinite order.

Thus, we have constructed an elliptic curve E of the form (1) with respect to the field Q of rational numbers, as well as a point B of infinite order on it. In order to construct a criptosystem by use of the pair (E, B), we can use a method described in [1]. To this end e.g. we choose a large prime number p and carry out the modulo p reduction of the curve and point B. The number p should be such that the reduced curve E' is elliptic over the field F_p. Taking into account the form of the curve (1), it is enough to require that p is greater than any integer involved in equation (1) as well as in the numerator and denominator of B. It is clear that the point B', the reduction of the point B, belongs to E'. Using the pair (E', B') as well as the results of [1] (Section 2 of Chapter VI) we can construct analogs of the well-known open key criptosystems (Diffi-Hellman, Messi-Omura, El-Gamal). The decoding complexity of the obtained criptosystems depends on the complexity of the problem of taking a discrete logarithm in the finite group E_p created by the F_p points belonging to the curve E'. The requirement that the point B should be of infinite order is stipulated by the following argument. If the order m of B is finite, according to the Mazur theorem, $m \leq 12$ [6]. For the order m' of the reduced point B' we also have $m' \leq 12$, and therefore the solution to the problem of finding discrete logarithm will not be complex, whereas when B is of infinite order, then the order of B' in E_p can be sufficiently large. If this is not the case, we can correct the order by means of the involved parameters p, a, b, r and s.

For the illustration of the above stated,we consider the following example. If we substitute in the formulas (3) and(4) the numbers $r = 2,\ s = 1,\ a = 5,\ b = 3,\ l = 1$, then we get that $n = 3990$, and the sides of triangles are $X = 133,\ Y = 120,\ Z = 127$. Because of $\cos\theta = 1/2$, we have that $n = 3990$ is $\pi/2$ congruent number and in this case the equation receives the following form

$$y^2 = x(x + 11970)(x - 3990)\ . \tag{8}$$

By use of formulas (7) we can construct the point $Q(x, y) = (-3591; 477603)$ lying on the curve (8). Let us consider the prime number $p = 97$ and reduce the equation (8) and the point Q on the field F_{97}. We obtain the equation

$$y^2 = x(x + 39)(x - 13) \tag{9}$$

and its point $P(x_1; y_1) = (95; 72)$. Assume now that two persons M and N have a desire to construct a code by means of the curve 8 defined over the field F_{97} and the point $P = (95; 72)$. For this purposes M remembers and preserves secretly e.g. the number $a = 6$, while N does the number $b = 4$. Using the well-known summation formulas given in [5], M and N find the following points on (8): $6P = (66; 40)$ and $4P = (62; 30)$ respectively, which are declared open. After that the both can get the number $4 \cdot 6P = 6 \cdot 4P = 24P = (11; 8)$, which will be open for them only. By use of the coordinates of this point, M and N are allowed to create a code. Let us note right away that in this example the order of the point $P(95; 72)$ is equal to 46.

Let us remark that in order to find a t-multiple of a point $P(x_1; y_1)$ of the curve, it is recommended first to find its a 2^d- multiple that $2^d \leq t < 2^{d+1}$.

Finding the point $2P$ in the case of curve (1) is being done by the formulas (see [5])

$$x_2 = -2x_1 - 2sn + (f'(x_1)/(2y_1))^2,$$

$$y_2 = -y_1 + (x_1 - x_2)f'(x_1)/(2y_1),$$

where $f(x)$ is the right-hand side of (1), i.e. $f'(x_1) = 3x_1^2 + 4snx - (r^2 - s^2)n^2$. Calculations give $x_2 = ((x_1^2 + (r^2 - s^2)n^2)/(2y_1))^2$. The use of the later frequently is practically convenient.

References

1. N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998.

2. M. Fujiwara, θ-congruent numbers, *in: Number Theory, K. Győry, A. Pethő, and V. Sós (eds.), de Gruyter,* (1997), 235-241.

3. M. Fujiwara, Some Properties of θ-Congruent Numbers, *Natural Science Report, Ochanomizu University,* **52** (2001), no.2, 1-8.

4. M. Kan, θ-Congruent Numbers and Elliptic Curves, *Acta Arithmetica*, vol. XCIV (2000), no.2, 153-160.

5. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

6. J.H. Silverman, J.Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.