

Re: Addition Law and K*P for Montgomery-form Curves

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-12/msg03727.html>

- *From:* "a\b" <a@xxx>
 - *Date:* Tue, 20 Dec 2005 11:36:03 +0100
-

On Tue, 20 Dec 2005 07:53:36 +0100, "a\b" <a@xxx> wrote:

>I have found this

>"

>1 Let

> $k = k_0 + k_1*2 + k_2*2^2 + \dots + k_r*2^r$; k_i in $[0; 1]$; $k_0 = k_r = 1$

>be the binary representation of k .

>

>2) Let $S = P$, $T = 2P$, $U = -P$.

>3) For $i = 1..r$ do the following:

> when $k_i = 1$

> $S := S + T$ (using U); $T := 2T$ (U is unchanged);

> when $k_i = 0$

> $U := U - T$ (using S); $T := 2T$ (S is unchanged):

>4) Then we have $S = kP$.

>"

>but if $k_0=1$ than k is odd: and for k even?

>There is someone that can post this algo in "coordinates form"

>or can explain what does it mean "using U " or $-P$ in a Montgomery-form

>Curve

>Thanks

if $P(x, 1, z)$ is a point in the Montgomery-form Curve

E: $b*Z*Y^2 = X^3 + a*Z*X^2 + X*Z^2$

what are the coordinates for $-P$?

Thank you

.

• *References:*

◆ [Addition Law and K*P for Montgomery-form Curves](#)

◇ *From:* a\b

• Prev by Date: [Re: Tesellating Circles](#)

• Next by Date: [Re: proof that inverse of continuous function is also continuous?](#)

• Previous by thread: [Addition Law and K*P for Montgomery-form Curves](#)

• Next by thread: [differentiability and derivative](#)

Re: Addition Law and K*P for Montgomery-form Curves

- Index(es):

- ◆ *Date*

- ◆ *Thread*