

Addition Law and K^*P for Montgomery-form Curves

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-12/msg03703.html>

- *From:* "a\b" <a@xxx>
 - *Date:* Tue, 20 Dec 2005 07:53:36 +0100
-

I have found this

"

1) Let

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

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 $k_0 \neq 1$ 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

.

• *Follow-Ups:*

◆ [Re: Addition Law and \$K^*P\$ for Montgomery-form Curves](#)

◇ *From:* a\b

• Prev by Date: [Structure of a semigroup](#)

• Next by Date: [Re: central forces](#)

• Previous by thread: [Structure of a semigroup](#)

• Next by thread: [Re: Addition Law and \$K^*P\$ for Montgomery-form Curves](#)

• Index(es):

◆ [Date](#)

◆ [Thread](#)