M. Montgomery curves

Consider the Weierstraß equation in its general form (A.1). For simplicity let us write y in place of x_2 and x in place of x_1. Suppose that $\mathrm{char}(K) \neq 2$. Then $y^2+a_1xy+a_3y = (y+(a_1x+a_3)/2)^2-(a_1x+a_3)^2/4$. Two Weierstraß equations are called *K-equivalent* if one can be obtained from the other by a linear substitution over K. The equation $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ is thus K-equivalent to the equation $y^2 = x^3+(a_2+a_1^2/4)x^2+(a_4+a_1a_3/2)x+(a_6+a_3^2/4)$, provided $\mathrm{char}(K) \neq 2$. Indeed, the latter equation can be turned into the equation (A.1) by $y \mapsto y+(a_1x+a_3)/2$ and $x \mapsto x$. (By a *linear substitution* over K we understand here any reversible substitution $x_i \mapsto \lambda_{1i}x_1+\lambda_{2i}x_2+\mu_i$, $i \in \{1,2\}$, where $\lambda_{ij}, \mu_i \in K$. Such a substitution is reversible if and only if $\det(\lambda_{ij}) \neq 0$.)

If $\mathrm{char}(K) > 3$, then $x^3+a_2x^2+a_4x+a_6 = (x+a_2/3)^3+(a_4-a_2^2/3)(x+a_2/3)+(a_6-a_4a_2/3+2a_2^3/27)$. Hence each Weierstraß equation is K-equivalent to a Weierstraß equation of the form $y^2 = x^3+ax+b$, provided $\mathrm{char}(K) > 3$.

A linear substitution may turn an equation $u(x,y) = v(x,y)$ into an equation $\lambda\tilde{u}(x,y) = \lambda\tilde{v}(x,y)$, where $\lambda \in K^*$. The curve determined by the latter equation is the same as the curve determined by $\tilde{u}(x,y) = \tilde{v}(x,y)$. Hence we say that $\tilde{u}(x,y) = \tilde{v}(x,y)$ is K-equivalent to $u(x,y) = v(x,y)$ also in this case.

If $\lambda \in K^*$, then the curve defined by the equation $y^2 = x^3+ax+b$ coincides with the curve given by $(\lambda^3y)^2 = (\lambda^2x)^3+a\lambda^4(\lambda^2x)+b\lambda^6$. The equation $y^2 = x^3+ax+b$ is hence K-equivalent to the equation $y^2 = x^3+\lambda^4ax+\lambda^6b$. This is the only way how Weierstraß equations $y^2 = x^3+ax+b$ and $y^2 = x^3+\tilde{a}x+\tilde{b}$ may be K-equivalent. They are K-equivalent if and only if

$$\text{there exists } \lambda \in K^* \text{ such that } \tilde{a} = \lambda^4 a \text{ and } \tilde{b} = \lambda^6 b. \tag{M.1}$$

Curves given by equations $By^2 = x^3+Ax^2+x$, $\mathrm{char}(K) \neq 2$, are also important. A curve of this form is called a *Montgomery curve*. We will also speak about a *Montgomery equation*. Elements A and B belong to K, and $B \neq 0$. Capital letters are used to avoid a confusion with a and b in the normal form of a Weierstraß equation.

When both sides of $By^2 = x^3+Ax^2+x$ are multiplied by B^3 we get

$$(B^2y)^2 = (Bx)^3+AB(Bx)^2+B^2(Bx).$$

A Montgomery equation is thus K-equivalent to a Weierstraß equation $y^2 = x^3+ABx^2+B^2x$. Weierstraß equations of the form $y^2 = f(x)$, $f \in K[x]$ cubic monic, $\mathrm{char}(K) \neq 2$, are smooth if and only if f is separable, i.e. it contains no multiple root. The polynomial $x(x^2+ABx+B^2)$ has a multiple root if and only if $(AB)^2-4B^2 = B^2(A-2)(A+2)$ is equal to zero. Hence if $A \neq \pm 2$, then the curve given by $y^2 = x^3+ABx^2+B^2x$ is smooth—and this is also, not surprisingly, the condition for the Montgomery curve to be smooth.

Assume $A \neq \pm 2$. Denote the Montgomery curve by M and the Weierstraß curve of $y^2 = x^3+ABx^2+B^2x$ by C. Note that $\sigma\colon (\alpha_1,\alpha_2) \mapsto (B\alpha_1, B^2\alpha_2)$ is a bijection $M \to C$. Extend this bijection by $\infty \mapsto \infty$. The group structure of $C(K)$ may be transferred upon M in such a way that $\sigma(\alpha) \oplus \sigma(\beta) = \sigma(\alpha \tilde{\oplus} \beta)$ for all $\alpha, \beta \in M \cup \{\infty\}$. This may be also written as $\alpha \tilde{\oplus} \beta = \sigma^{-1}(\sigma(\alpha) \oplus \sigma(\beta))$ for all $\alpha, \beta \in M \cup \{\infty\}$.

Suppose that $\alpha = (\alpha_1, \alpha_2)$. Then

$$\tilde{\ominus}\alpha = \sigma^{-1}(\ominus(B\alpha_1, B^2\alpha_2)) = \sigma^{-1}(B\alpha_1, -B^2\alpha_2) = (\alpha_1, -\alpha_2).$$

The formula for opposite elements thus does not change, and so we can write $\ominus$ in place of $\tilde{\ominus}$ when the unary minus is being used.

The value of λ for $(B\alpha_1, B^2\alpha_2) \oplus (B\beta_1, B^2\beta_2)$ comes from (A.3) as

$$\frac{3B^2\alpha_1^2 + 2AB^2\alpha_1 + B^2}{2B^2\alpha_2} = \frac{3\alpha_1^2 + 2A\alpha_1 + 1}{2\alpha_2} \text{ if } \alpha = \beta, \text{ and } B\frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \text{ if } \alpha \neq \beta.$$

Assume that $\alpha \neq \ominus\beta$, and set $\gamma = \alpha\tilde{\oplus}\beta$, $\gamma = (\gamma_1, \gamma_2)$. By (A.4),

$$(\gamma_1, \gamma_2) = (-\alpha_1 - \beta_1 + B^{-1}\lambda^2 - A, B^{-1}\lambda(\alpha_1 - \gamma_1) - \alpha_2).$$

Let us express the latter formula using $\tilde{\lambda} = B^{-1}\lambda$. Note that $\tilde{\lambda}$ expresses the slope of the line connecting α and β, if $\alpha \neq \beta$. Indeed,

$$\tilde{\lambda} = \frac{3\alpha_1^2 + 2A\alpha_1 + 1}{2B\alpha_2} \text{ if } \alpha = \beta, \quad \tilde{\lambda} = \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \text{ if } \alpha \neq \beta, \text{ and} \tag{M.2}$$

$$(\gamma_1, \gamma_2) = (-\alpha_1 - \beta_1 + B\tilde{\lambda}^2 - A,\ \tilde{\lambda}(\alpha_1 - \gamma_1) - \alpha_2). \tag{M.3}$$

Assume $\alpha_1 \neq \beta_1$ and use the fact that $\alpha\tilde{\ominus}\beta = \alpha\tilde{\oplus}(\beta_1, -\beta_2)$. Let $\alpha\tilde{\ominus}\beta = \delta = (\delta_1, \delta_2)$. By (M.3),

$$(\delta_1, \delta_2) = (-\alpha_1 - \beta_1 + B\tilde{\tilde{\lambda}}^2 - A, \tilde{\tilde{\lambda}}(\alpha_1 - \delta_1) - \alpha_2), \text{ where } \tilde{\tilde{\lambda}} = \frac{\alpha_2 + \beta_2}{\alpha_1 - \beta_1}. \tag{M.4}$$

Proposition M.1. *Let $\tilde{\oplus}$ be the group operation upon a Montgomery curve M given over K by $By^2 = x^3 + Ax^2 + x$. Let $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$ be K-rational points of M, $\alpha_1 \neq \beta_1$. Put $\gamma = \alpha\tilde{\oplus}\beta = (\gamma_1, \gamma_2)$ and $\delta = \alpha\tilde{\ominus}\beta = (\delta_1, \delta_2)$. Then*

$$\gamma_1\delta_1(\alpha_1 - \beta_1)^2 = (\alpha_1\beta_1 - 1)^2. \tag{M.5}$$

Proof. Start with (M.3) and express $B\alpha_2^2$ and $B\beta_2^2$ by means of the Montgomery equation to get

$$\begin{aligned}
\gamma_1(\alpha_1 - \beta_1)^2 &= B(\alpha_2 - \beta_2)^2 - (A + \alpha_1 + \beta_1)(\alpha_1 - \beta_1)^2 \\
&= -2B\alpha_2\beta_2 + (\alpha_1^3 + A\alpha_1^2 + \alpha_1) + (\beta_1^3 + A\beta_1^2 + \beta_1) \\
&\quad - \alpha_1^3 - \beta_1^3 + \alpha_1^2\beta_1 + \alpha_1\beta_1^2 - A\alpha_1^2 - A\beta_1^2 + 2A\alpha_1\beta_1 \\
&= -2B\alpha_2\beta_2 + \alpha_1\beta_1(\alpha_1 + \beta_1 + 2A) + \alpha_1 + \beta_1.
\end{aligned}$$

Therefore

$$\begin{aligned}
\gamma_1(\alpha_1 - \beta_1)^2\alpha_1\beta_1 &= -2B\alpha_2\beta_2\alpha_1\beta_1 + \beta_1^2(\alpha_1^3 + A\alpha_1^2 + \alpha_1) + \alpha_1^2(\beta_1^3 + A\beta_1^2 + \beta_1) \\
&= -2B\alpha_1\beta_1\alpha_2\beta_2 + B\beta_1^2\alpha_2^2 + B\alpha_1^2\beta_2^2 = B(\beta_1\alpha_2 - \beta_2\alpha_1)^2.
\end{aligned}$$

The right hand side of (M.4) is obtained from the right hand side of (M.3) by replacing β_2 with $-\beta_2$. Hence we have

$$\begin{aligned}
\gamma_1(\alpha_1 - \beta_1)^2\alpha_1\beta_1 &= B(\beta_1\alpha_2 - \beta_2\alpha_1)^2 \text{ and} \\
\delta_1(\alpha_1 - \beta_1)^2\alpha_1\beta_1 &= B(\beta_1\alpha_2 + \beta_2\alpha_1)^2.
\end{aligned} \tag{M.6}$$

By multiplying, $\gamma_1\delta_1(\alpha_1 - \beta_1)^4\alpha_1^2\beta_1^2 = B^2(\beta_1^2\alpha_2^{2\text{‘}} - \beta_2^2\alpha_1^2)^2$. Now,

$$\begin{aligned}
B(\beta_1^2\alpha_2^2 - \beta_2^2\alpha_1^2) &= \beta_1^2(\alpha_1^3 + A\alpha_1^2 + \alpha_1) - \alpha_1^2(\beta_1^2 + A\beta_1^2 + \beta_1) \\
&= (\alpha_1\beta_1)^2(\alpha_1 - \beta_1) + \alpha_1\beta_1(\beta_1 - \alpha_1) = (\alpha_1 - \beta_1)\alpha_1\beta_1(\alpha_1\beta_1 - 1).
\end{aligned}$$

Hence $\gamma_1\delta_1(\alpha - \beta_1)^4(\alpha_1\beta_1)^2 = (\alpha_1\beta_1)^2(\alpha - \beta_1)^2(\alpha_1\beta_1 - 1)^2$, and so

$$\gamma_1\delta_1(\alpha_1 - \beta_1)^2 = (\alpha_1\beta_1 - 1)^2.$$

This yields (M.5) if $\alpha_1\beta_1 \neq 0$. If $\beta_1 = 0$, then $\beta_2 = 0$, $\gamma_1 = \delta_1 = -\alpha_1 + B\alpha_2^2\alpha_1^{-2} - A$ and $\alpha_1^2\gamma_1 = -\alpha_1^3 + B\alpha_2^2 - A\alpha_1^2 = \alpha_1$. Thus $\alpha_1\gamma_1 = \alpha_1\delta_1 = 1$, and both sides of (M.5) are equal to 1.

If $\alpha_1 = 0$, then $\alpha_2 = 0$, $\gamma_1 = -\beta_1 + B\beta_2^2\beta_1^{-2} - A = \delta_1$ and $\gamma_1\beta_1^2 = -\beta_1^3 + B\beta_2^2 - A\beta_1^2 = \beta_1$. Hence $\gamma_1\beta_1 = \delta_1\beta_1 = 1$, and both sides of (M.5) are equal to 1 again. □

There exists a natural technique how to compute $[n]P$ by means of a sequence $1 = n_1, \ldots, n_k$ of integers such that in the ith round both $[n_i]P$ and $[n_i+1]P$ are known. This is known as *Montgomery's ladder* and is discussed below. If $\beta = [n_i]P$ and $\alpha = [n_i + 1]P$, then $\alpha \tilde{\ominus} \beta = P$. Hence (M.5) may be used to obtain $\gamma = \alpha \tilde{\oplus} \beta = [2n_i + 1]P$. The practicality of such a procedure follows from the fact that we may work only in the first coordinate. For all $[n_i]P$ and $[n_i + 1]P$ only the first coordinate is being computed, and the second coordinate of $[n]P$ is retrieved from the last two elements of the sequence, cf. Lemma M.2.

Since Montgomery's ladder needs also doubling, we have to verify that doubling can be performed in the first coordinate only too:

Let $(\gamma_1, \gamma_2) = [2]\alpha$, where $\alpha = (\alpha_1, \alpha_2)$ and $\alpha_2 \neq 0$. By (M.2) and (M.3), γ_1 is equal to $-2\alpha_1 - A + B(3\alpha_1^2 + 2A\alpha_1 + 1)^2(2B\alpha_2)^{-2}$. Thus

$$\begin{aligned} 4B\gamma_1\alpha_2^2 &= -8\alpha_1(B\alpha_2^2) + (3\alpha_1^2 + 2A\alpha_1 + 1)^2 - 4A(B\alpha_2^2) \\ &= -(8\alpha_1 + 4A)(\alpha_1^3 + A\alpha_1^2 + \alpha_1) + 9\alpha_1^4 + 12A\alpha_1^3 + (6 + 4A^2)\alpha_1^2 + 4A\alpha_1 + 1 \\ &= \alpha_1^4 - 2\alpha_1^2 + 1. \end{aligned}$$

Hence

$$\gamma_1 = \frac{(\alpha_1^2 - 1)^2}{4B\alpha_2^2} = \frac{(\alpha_1^2 - 1)^2}{4(\alpha_1^3 + A\alpha_1^2 + \alpha_1)}. \tag{M.7}$$

In the context of Montgomery's ladder the points occurring in the following statement have this meaning: $\gamma = [n + 1]P$, $\alpha = [n]P$ and $\beta = P \neq (0, 0)$. The goal is to determine α_2 from knowledge of α_1, γ_1, β_1 and β_2.

Lemma M.2. *Let $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$ and $\gamma = (\gamma_1, \gamma_2)$ be points of a Montgomery curve over K given by $By^2 = x^3 + Ax^2 + x$. Suppose that $\alpha_1 \neq \beta_1$, $\beta \neq (0, 0)$ and that $\gamma = \alpha \tilde{\oplus} \beta$, where $\tilde{\oplus}$ is the group operation upon $M \cup \{\infty\}$. Then*

$$\alpha_2 = \frac{\alpha_1\beta_1(\alpha_1 + \beta_1 + 2A) + \alpha_1 + \beta_1 - \gamma_1(\alpha_1 - \beta_1)^2}{2B\beta_2}$$

Proof. The first equation in the proof of Proposition M.1 is

$$\gamma_1(\alpha_1 - \beta_1)^2 = -2B\alpha_2\beta_2 + \alpha_1\beta_1(\alpha_1 + \beta_1 + 2A) + \alpha_1 + \beta_1.$$

It remains to express α_2 using this equation. □

M.1. **Montgomery's ladder.** Let us start by an example. The binary expansion of, say, $n = 49$ is 110001 since $49 = 32 + 16 + 1$. The decimal expression of binary integers 1, 11, 110, 1100, 11000 and 110001 is 1, 3, 6, 12, 24 and 49. Put $n_1 = 1$, $n_2 = 3$, $n_3 = 6$, $n_4 = 12$, $n_5 = 24$ and $n_6 = 49$, and set $n_i' = n_i + 1$, $1 \leq i \leq 6$. Note that $(3, 4) = (1 + 2, 2 + 2)$, $(6, 7) = (3 + 3, 3 + 4)$, $(12, 13) = (6 + 6, 6 + 7)$, $(24, 25) = (12 + 12, 12 + 13)$ and $(49, 50) = (24 + 25, 25 + 25)$. Obviously there are two patterns. Either $(n_{i+1}, n_{i+1}') = (2n_i, n_i + n_i')$, or $(n_{i+1}, n_{i+1}') = (n_i + n_i', 2n_i')$. The former equality holds if the rightmost bit of n_{i+1} is equal to 0, while the latter equality holds if the rightmost bit of n_{i+1} is equal to 1. This will be proved below.

Now suppose that our goal is to compute $[n]P$, $P \neq (0, 0)$ a point of a Montgomery curve M. Let $x_i, y_i, x_i', y_i' \in K$ be such that $[n_i]P = (x_i, y_i)$ and $[n_i']P = (x_i', y_i')$. The sequence $n_1, n_2, \ldots, n_k$ is defined so that $n_k = n$. Thus $[n]P = (x_k, y_k)$.

The recommended procedure is to compute x_i and x_i' by means of (M.5) and (M.7), and then use Lemma M.2 to retrieve y_k from knowledge of x_k, x_k', and $P = (x_1, y_1)$.

Let us be more concrete. Suppose first that $(n_{i+1}, n_{i+1}') = (2n_i, n_i + n_i')$. Then

$$x_{i+1} = \frac{(x_i^2 - 1)^2}{4(x_i^3 + Ax_i^2 + x_i)}, \text{ and } x_{i+1}' = \frac{(x_ix_i' - 1)^2}{x_1(x_i' - x_i)^2}. \tag{M.8}$$

If $(n_{i+1}, n'_{i+1}) = (n_i + n'_i, 2n'_i)$, then

$$x_{i+1} = \frac{(x_i x'_i - 1)^2}{x_1(x'_i - x_i)^2}, \text{ and } x'_{i+1} = \frac{(x'^2_i - 1)^2}{4(x'^3_i + Ax'^2_i + x'_i)}. \tag{M.9}$$

Finally, by Lemma M.2,

$$y_k = \frac{x_1 x_k(x_1 + x_k + 2A) + x_1 + x_k - x'_k(x_k - x_1)^2}{2By_1}.$$

Of course, the scheme assumes that the order of P is greater than $n + 1$. Thus $[m]P \neq \infty$ for any m, $1 \leq m \leq n + 1$.

When implementing the arithmetic of Montgomery curves the effeciency may be enhanced by using projective coordinates.

Let us formalize observations deduced from the initial example. Note that if $n = \sum_{0 \leq i < k} a_i 2^i$ is a binary expansion of n (thus $a_i \in \{0, 1\}$ and $a_{k-1} = 1$), then the sequence n_1, n_2, ..., n_k constructed above can be expressed as $n_1 = 1$, $n_2 = 2 + a_{k-2} = 2a_{k-1} + a_{k-2}$, $n_3 = 4a_{k-1} + 2a_{k-2} + a_{k-3}$, etc. Thus $n_j = \sum_{1 \leq i \leq j} a_{k-i} 2^{j-i}$.

Lemma M.3. *Let $n \geq 1$ be an integer, and let $\sum_{0 \leq i < k} a_i 2^i$ be its binary expansion, $a_{k-1} = 1$. For $j \in \{1, \ldots, k\}$ define n_j as $\sum_{1 \leq i \leq j} a_{k-i} 2^{j-i}$, and put $n'_j = n_j + 1$. Then $n_1 = 1$, $n_k = n$, and for every j, $1 \leq j < k$ the following holds:*

- *If $a_{k-j-1} = 0$, then $n_{j+1} = 2n_j$ and $n'_{j+1} = n_j + n'_j$.*
- *If $a_{k-j-1} = 1$, then $n_{j+1} = n_j + n'_j$ and $n'_{j+1} = 2n'_j$.*

Proof. Put $\varepsilon = a_{k-j-1}$. By the definition, $n_{j+1} = 2n_j + \varepsilon$. If $\varepsilon = 0$, then $n_{j+1} = 2n_j$. If $\varepsilon = 1$, then $n_{j+1} + 1 = 2(n_j + 1)$. □

M.2. **Turning Weierstraß into Montgomery.** Recall that by multiplying the equation $By^2 = x^3 + Ax^2 + x$ by B^3 we obtain a K-equivalent Weierstraß equation $y^2 = x^3 + ABx^2 + B^2x$. Hence we may immediately claim the following fact:

Lemma M.4. *A Weierstraß equation $y^2 = f(x)$, where $f(x) = x^3 + a_2x^2 + a_4x + a_6$, is K-equivalent to a Montgomery equation if and only if it is K-equivalent to a Weierstraß equation $y^2 = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x$ in which $\tilde{a}_4$ is in K a nonzero square.*

Assume $\mathrm{char}(K) > 3$. Expressing $x^3 + ABx^2 + B^2x$ as a polynomial in $x + AB/3$ shows that $By^2 = x^3 + Ax^2 + x$ is K-equivalent to

$$y^2 = x^3 + B^2\left(1 - \frac{A^2}{3}\right)x - \frac{AB^3}{3} + \frac{2(AB)^3}{27}. \tag{M.10}$$

If $y^2 = x^3 + ax + b$, then it may not be easy to decide whether there exist A and B such that $a = B^2(1 - A^2/3)$ and $b = -(AB^3)/3 + 2(AB)^3/27$. The following structural description may be then useful.

Proposition M.5. *A Weierstraß equation $y^2 = f(x)$ is K-equivalent to a Montgomery equation if and only if there exists $\zeta \in K$ such that $f(\zeta) = 0$ and $f'(\zeta)$ is in K a nonzero square.*

Proof. If $f(x) = x^3 + ABx^2 + B^2x$, then $f'(x) = 3x^2 + 2ABx + B^2$, $f(0) = 0$ and $f'(0) = B^2$. For the converse direction suppose that $y^2 = f(x)$, $f'(\zeta) = B^2$ and $f(\zeta) = 0$. Put $\tilde{f}(x) = f(x + \zeta)$. Then $\tilde{f}(x) = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$, and $\tilde{a}_6 = \tilde{f}(0) = f(\zeta) = 0$. Furthermore, $\tilde{a}_4 = \tilde{f}'(0) = f'(\zeta)$ is assumed to be square. The equation $y^2 = \tilde{f}(x)$ is thus equivalent to a Montgomery equation, by Lemma M.4.

To finish the proof we have to show that if $y^2 = f(x)$ and $y^2 = \tilde{f}(x)$ are K-equivalent Weierstraß equations, then from the existence of ζ with $f(\zeta) = 0$ and $f'(\zeta) \in (K^*)^2$ there follows the existence of $\tilde{\zeta}$ with the same properties. (This part

of the proof is necessary since without it there would remain open a possibility that a Montgomery equation is K-equivalent to a Weierstraß equation that does not have the required property.) If $\tilde{f}(x) = f(x + \mu)$, set $\tilde{\zeta} = \zeta - \mu$. If $\tilde{f}(x)$ is obtained from $f(\lambda_1 x)$, $\lambda_1 \in K^*$, then λ_1 must be a square (cf. the discussion before (M.1)). Suppose that $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Then $\lambda^6 y^2 = (\lambda^2 x)^3 + a_2\lambda^2(\lambda^2 x)^2 + a_4\lambda^4(\lambda^2 x) + a_6\lambda^6$. Thus $\tilde{f}(x) = x^3 + a_2\lambda^2 x^2 a + a_4\lambda^4 x + a_6\lambda^6$. Put $\tilde{\zeta} = \lambda^2\zeta$. Then $\tilde{f}(\tilde{\zeta}) = \lambda^6 f(\zeta) = 0$, and $\tilde{f}'(\tilde{\zeta}) = 3\tilde{\zeta}^2 + 2a_2\lambda^2\tilde{\zeta} + a_4\lambda^4 = \lambda^4(3\zeta^2 + 2a_2\zeta + a_4) = \lambda^4(f'(\zeta))$ is a square. □

Corollary M.6. *Let $p \equiv 1 \bmod 4$ be a prime, and let $f \in \mathbb{Z}_p[x]$ be a cubic monic separable polynomial that splits over $\mathbb{Z}_p$ (i.e. all roots of f are in $\mathbb{Z}_p$). If $f(0) \neq 0$, then the Weierstraß equation $y^2 = f(x)$ is K-equivalent to a Montgomery equation.*

Proof. By the assumptions, $f(x) = (x - \zeta_1)(x - \zeta_2)(x - \zeta_3)$, where $\zeta_i \in \mathbb{Z}_p$. We have

$$-\prod f'(\zeta_i) = \prod_{i<j} (\zeta_i - \zeta_j)^2.$$

This is because both sides of the equality express the discriminant of f. (This equality can be also verified directly, which is an option for those who are not familiar with discriminants.) Because -1 is modulo p a square, $\prod f'(\zeta_i)$ is also a square. Therefore at least one of $f'(\zeta_i)$ has to be a square too. □

It is not difficult to solve completely the question when two Montgomery equations are K-equivalent. Here we shall restrict our attention only to the fact that $By^2 = x^3 + Ax^2 + x$ holds if and only if $-By^2 = (-x)^3 - A(-x)^2 + (-x)$. A Montgomery equation with parameters (A, B) is hence K-equivalent to a Montgomery equation with parameters $(-A, -B)$.