

Arithmetic of Genus 2 Real Hyperelliptic Curve

$$y^2 + (h_3 x^3 + h_2 x^2 + h_1 x + h_0) \cdot y = f_6 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

If the characteristic of k is not 2, then $h(x) = 0$. If the characteristic of k is not 3, then $f_5 = 0$. If the characteristic of k is 2 and $f_6 = 1$ (which is possible if and only the number of elements in k is an even power of 2), then $h_3 = 1$ and $h_2 = f_5 = f_4 = f_3 = 0$.

$$\begin{aligned} inv &\equiv r(u_2)^{-1} \pmod{u_1} & s' &= rs = inv \cdot (v_1 - v_2) \pmod{u_1} \\ k &= \frac{f - h \cdot v_2 - v_2^2}{u_2} & l &= s \cdot u_2 \\ m &= k - s \cdot (l + h + 2v_2) & m' &= m/m_4 = m \text{ made monic} \\ u' &= m'/u_1 & v' &= h - v_2 - l \pmod{u'} \end{aligned}$$

Addition, Adapted Basis, $\deg u_1 = \deg u_2 = 2$, $\gcd(u_1, u_2) = 1$		
Input	$u_1 = x^2 + u_{11}x + u_{10}, v_1 = v_{11}x + v_{10}$ $u_2 = x^2 + u_{21}x + u_{20}, v_2 = v_{21}x + v_{20}$	
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$	
Step	Expression	# of Operations
Composition		
1	$inv = z_1x + z_2$ $z_0 = u_{10} - u_{20}, z_1 = u_{11} - u_{21}, z_2 = u_{11} \cdot z_1 - z_0$ $w_0 = v_{10} - v_{20}, w_1 = v_{11} - v_{21}, r = z_1 \cdot (z_1 \cdot u_{10}) - z_0 \cdot z_2$	4M
2	$s' = s'_1x + s'_0$ $s'_1 = w_0 \cdot z_1 - w_1 \cdot z_0, s'_0 = w_0 \cdot z_2 - w_1 \cdot (z_1 u_{10})$	4M
Reduction		
3	$k = k_4x^4 + k_3x^3 + k_2x^2 + k_1x + k_0$ $k_4 = f_6, k_3 = f_5 - f_6u_{21}, k_2 = f_4 - h_3v_{21} - f_6u_{20} - f_5u_{21} + f_6u_{21}^2$	1S
4	$s = \frac{s'}{r} = s_1x + s_0$ $\tilde{m}_4 = f_6r^2 - s'_1 \cdot (s'_1 + h_3r), I = (r \cdot \tilde{m}_4)^{-1},$ $\frac{1}{r} = \tilde{m}_4 \cdot I, s_1 = s'_1 \cdot \frac{1}{r}, s_0 = s'_0 \cdot \frac{1}{r}, \frac{1}{m_4} = r \cdot r^2 \cdot I$	1I, 2S, 6M (1I, 1S, 7M)
5	$l = l_3x^3 + l_2x^2 + l_1x + l_0$ $\tilde{w}_0 = s_0 \cdot u_{20}, \tilde{w}_1 = s_1 \cdot u_{21}, l_3 = s_1, l_2 = s_0 + \tilde{w}_1$ $l_1 = (s_0 + s_1) \cdot (u_{21} + u_{20}) - \tilde{w}_1 - \tilde{w}_0, l_0 = \tilde{w}_0$	3M
6	$m' = x^4 + m'_3x^3 + m'_2x^2 + m'_1x + m'_0, u' = x^2 + u'_1x + u'_0$ $m'_3 = \frac{m_3}{m_4} = (\frac{1}{m_4}) \cdot (k_3 - s_1 \cdot (s_0 + l_2 + h_2) - h_3s_0)$ $m'_2 = \frac{m_2}{m_4} = (\frac{1}{m_4}) \cdot (k_2 - s_1 \cdot (l_1 + h_1 + 2v_{21}) - s_0 \cdot (l_2 + h_2))$ $u'_1 = m'_3 - u_{11}, u'_0 = m'_2 - u_{10} - u_{11} \cdot u'_1$	6M
7	$v' = v'_1x + v'_0$ $v'_3 = h_3 - l_3, \underline{w}_1 = u'_1 \cdot v'_3, v'_2 = h_2 - l_2 - \underline{w}_1, \underline{w}_0 = u'_0 \cdot v'_2$ $v'_1 = h_1 - v_{21} - l_1 - (u'_0 + u'_1) \cdot (v'_2 + v'_3) + \underline{w}_0 + \underline{w}_1, v'_0 = h_0 - v_{20} - l_0 - \underline{w}_0$	3M
Total		1I, 3S, 26M (1I, 2S, 27M)

We don't count multiplication by f_6 and h_3 , which almost always can be assumed to be either 0 or 1. Also, h_2 can always be assumed to be 0, and f_5 may assumed to be 0 if $\text{char } k \neq 3$. We leave them in the formulas for completeness. Also, it shown below that we can save one squaring in the reduced basis $v_i = x^3 + v_{i1}x + v_{i0}$ in odd characteristic when calculating k_2 .

For the reduced basis, we make the following modifications (assuming $f_6 = 1$ and $f_5 = 0$ in odd characteristic and $h_3 = f_6 = 1$ and $h_2 = f_5 = f_4 = 0$ in even characteristic):

1. In Step 3, let $k_4 = 0$, $k_3 = 0$, $k_4 = f_4 - 2v_{21}$ in odd characteristic, and let $k_4 = 1$, $k_3 = u_{21}$, $k_2 = h_1 + v_{21} + u_{20} + u_{21}^2$ in even characteristic.
2. In Step 4, let $\tilde{m}_4 = r^2 - (s'_1 + r)^2$ in odd characteristic, and let $\tilde{m}_4 = r^2 + s'_1 \cdot (s'_1 + r)$ in even characteristic.
3. In Step 7, let $v'_3 = h_3 - l_3 - 2$.

In odd characteristic, the modification in Step 3 saves one squaring. The total number of field operations for the reduced basis in odd characteristic is 1 inversion, 2 squares, and 26 multiplications. The number of operations for the reduced basis in even characteristic is the same as the adapted basis, 1 inversion, 2 squares, and 27 multiplications.

Cantor's Algorithm for Real Case

Let (u_1, v_1) and (u_2, v_2) be two reduced divisors written in the Mumford representation. Assume u_1 and u_2 are both degree 2 and are relatively prime. The composition step of Cantor's Algorithm is given by

$$\begin{aligned} U_0 &= u_1 u_2 \\ V_0 &\equiv v_2 + s u_2 = v_2 + l \pmod{U_0} \end{aligned}$$

where $s \equiv u_2^{-1} \cdot (v_1 - v_2) \pmod{u_1}$ and $l = s u_2$. The reduction step is given by

$$\begin{aligned} V_1 &= h - V_0 + \left\lfloor \frac{V_0 + d}{U_0} \right\rfloor \cdot U_0 \\ U_1 &= \frac{f + h \cdot V_1 - V_1^2}{U_0} \end{aligned}$$

where $d(x)$ is the principal part of a root of the equation $y^2 + h(x) \cdot y = f(x)$. Since V_0 and d both have degree 3 and U_0 has degree 4, $\left\lfloor \frac{V_0 + d}{U_0} \right\rfloor = 0$, and so

$$V_1 = h - V_0 = h - (v_2 + l)$$

Plugging this into the formula U_1 and noting that either $h = 0$ in odd characteristic or $2 = 0$ in even characteristic,

$$\begin{aligned} U_1 &= \frac{f + h(h - (v_2 + l)) - (h - (v_2 + l))^2}{u_1 u_2} \\ &= \frac{f - h v_2 - h l - v_2^2 - l^2 - 2 v_2 l}{u_1 u_2} \\ &= \frac{1}{u_1} \left(\frac{f - h v_2 - v_2}{u_2} - \frac{l(h + l + 2 v_2)}{u_2} \right) \\ &= \frac{k - s(h + l + 2 v_2)}{u_1} \end{aligned}$$

where $k = \frac{f - h v_2 - v_2}{u_2}$.

Composition

$inv = z_1x + z_2$, 4M

We can skip the calculation of U_0 . We do need to calculate s , and consequently l . The first step is to calculate $inv = u_2^{-1} \pmod{u_1}$. Let $z_0 = u_{10} - u_{20}$, $z_1 = u_{11} - u_{21}$, $z_2 = u_{11} \cdot z_1 - z_0$, and $r = z_1 \cdot (z_1 \cdot u_{10}) - z_0 \cdot z_2$. By the Euclidean algorithm,

$$\begin{aligned} u_2 &= u_1 - (z_1x + z_0) \\ u_1 &= (z_1^{-1})^2(z_1x + z_2)(z_1x + z_0) + (z_1^{-1})^2r \end{aligned}$$

Solving for the constant term, we have

$$(z_1^{-1})^2r = (1 - (z_1^{-1})^2inv)u_1 + ((z_1^{-1})^2inv)u_2 \equiv ((z_1^{-1})^2inv)u_2 \pmod{u_1}$$

Hence, inv is the constant r times the inverse of u_2 modulo u_1 .

$s' = s'_1x + s_0$, 4M

We next calculate $s' = rs \equiv inv(v_1 - v_2) \pmod{u_1}$. Let $w_0 = v_{10} - v_{20}$ and $w_1 = v_{11} - v_{21}$. Then

$$\begin{aligned} s' &= inv(v_1 - v_2) = (z_1x + z_2)(w_1x + w_0) \\ &= (w_1z_1)x^2 + (w_1z_2 + w_0z_1)x + (w_0z_2) \\ &\equiv (w_1z_2 + w_0z_1 - u_{11}w_1z_1)x + (w_0z_2 - u_{10}w_1z_1) \\ &\equiv (w_1((u_{11}z_1 - z_0) - u_{11}z_1) + w_0z_1)x + (w_0z_2 - u_{10}w_1z_1) \\ &\equiv (w_0z_1 - w_1z_0)x + (w_0z_2 - w_1z_1u_{10}) \pmod{u_2} \end{aligned}$$

Hence, if $s' = s'_1x + s'_0$, then $s'_1 = w_0 \cdot z_1 - w_1 \cdot z_0$ and $s'_0 = w_0 \cdot z_2 - w_1 \cdot (z_1u_{10})$. We note that $z_1 \cdot u_{10}$ is calculated before in r , so this saves one squaring in the calculation. This improvement applies to the imaginary formulas as well.

Reduction

$k = k_4x^4 + k_3x^3 + k_2x^2 + \dots$

We first calculate the first three coefficients of $k = \frac{f + hv_2 - v_2^2}{u_2}$. By the conditions on the Mumford representation, the division in the definition of k is exact.

Adapted Basis ($v_2 = v_{21}x + v_{20}$), 1S

$$\begin{aligned} k &= \frac{(f_6x^6 + f_5x^5 + f_4x^4 + \dots) + (h_3x^3 + h_2x^2 + h_1x + h_0)(v_{21}x + v_{20}) - (v_{21}x + v_{20})^2}{x^2 + u_{21}x + u_{20}} \\ &= \frac{f_6x^6 + f_5x^5 + (f_4 + h_3v_{21})x^4 + \dots}{x^2 + u_{21}x + u_{20}} \\ &= f_6x^4 + (f_5 - f_6u_{21})x^3 + (f_4 + h_3v_{21} - f_6u_{20} - (f_5 - f_6u_{21}) \cdot u_{21})x^2 + \dots \end{aligned}$$

Hence, $k_4 = f_6$ (which is usually 1), $k_3 = f_5 - f_6u_{21}$ (which is usually $-u_{21}$), and $k_2 = f_4 + h_3v_{21} + f_6(u_{21}^2 - u_{20}) - f_5u_{21}$.

Reduced Basis ($v_2 = x^3 + v_{21}x + v_{20}$), **(Even: 1S)**

$$\begin{aligned}
k &= \frac{(f_6x^6 + f_5x^5 + f_4x^4 + \dots) + (h_3x^3 + h_2x^2 + h_1x + h_0)(x^3 + v_{21}x + v_{20}) - (x^3 + v_{21}x + v_{20})^2}{x^2 + u_{21}x + u_{20}} \\
&= \frac{(f_6 + h_3 - 1)x^6 + (f_5 + h_2)x^5 + (f_4 + h_1 + (h_3 - 2)v_{21})x^4 + \dots}{x^2 + u_{21}x + u_{20}} \\
&= \underbrace{(f_6 + h_3 - 1)}_{k_4} x^4 + \underbrace{(f_5 + h_2 - k_4 u_{21})}_{k_3} x^3 + (f_4 + h_1 + (h_3 - 2)v_{21} - k_4 u_{20} - k_3 u_{21})x^2 + \dots
\end{aligned}$$

If the characteristic is not 2 or 3, we may assume $f_6 = 1$ and $f_5 = 0$. Then $k_4 = k_3 = 0$ and $k_2 = f_4 - 2v_{21}$. In even characteristic and assuming $f_6 = h_3 = 1$, $f_5 = f_4 = h_2 = 0$, then $k_4 = 1$, $k_3 = u_{21}$, $k_2 = h_1 + v_{21} + u_{20} + u_{21}^2$.

$$m = m_4x^4 + m_3x^3 + m_2x^2 + \dots$$

We now calculate the numerator $m = k - s(l + h + 2v_2)$ of U_1 , the reduction of $U_0 = u_1u_2$. What we really need is $u' = \frac{m}{u_1}$ made monic, which means we must invert the leading coefficient m_4 . We leave the coefficients in most general terms for now.

Adapted Basis ($v_2 = v_{21}x + v_{20}$), **2S (Even: 1M, 1S)**

$$\begin{aligned}
m &= (k_4x^4 + k_3x^3 + k_2x^2 + \dots) - (s_1x + s_0)((l_3 + h_3)x^3 + (l_2 + h_2)x^2 + (l_1 + h_1 + 2v_{21})x + \dots) \\
&= (k_4 - s_1(l_3 + h_3))x^4 + (k_3 - s_1(l_2 + h_2) - s_0(l_3 + h_3))x^3 \\
&\quad + (k_2 - s_1(l_1 + h_1 + 2v_{21}) - s_0(l_2 + h_2))x^2 + \dots
\end{aligned}$$

Plugging in $k_4 = f_6$ and $l_3 = s_1$, we have $m_4 = f_6 - s_1(s_1 + h_3)$. Since only $s'_1 = r s_1$ is known, we multiply m_4 by r^2 :

$$\tilde{m}_4 = r^2 m_4 = f_6 r^2 - s'_1 (s'_1 + h_3 r)$$

In odd characteristic, $\tilde{m}_4 = r^2 - s'^2_1$. In even characteristic, $\tilde{m}_4 = r^2 + s'_1 \cdot (s'_1 + r)$.

Reduced Basis ($v_2 = x^3 + v_{21}x + v_{20}$), **2S (Even: 1M, 1S)**

$$\begin{aligned}
m &= (k_4x^4 + k_3x^3 + k_2x^2 + \dots) - (s_1x + s_0)((l_3 + h_3 + 2)x^3 + (l_2 + h_2)x^2 + (l_1 + h_1 + 2v_{21})x + \dots) \\
&= (k_4 - s_1(l_3 + h_3 + 2))x^4 + (k_3 - s_1(l_2 + h_2) - s_0(l_3 + h_3 + 2))x^3 \\
&\quad + (k_2 - s_1(l_1 + h_1 + 2v_{21}) - s_0(l_2 + h_2))x^2 + \dots
\end{aligned}$$

In odd characteristic, $m_4 = k_4 - s_1(l_3 + h_3 + 2) = -s_1(s_1 + 2)$ and

$$\tilde{m}_4 = r^2 m_4 = r^2 - (s'_1 + r)^2$$

Note that we need r^2 in the next step, which is why we write m_4 in this way. In even characteristic (assuming $f_6 = 1$), $m_4 = 1 + s_1 \cdot (s_1 + 1)$ and

$$\tilde{m}_4 = r^2 m_4 = r^2 + s'_1 \cdot (s'_1 + r)$$

Inverse Step, $I = (r \cdot \tilde{m}_4)^{-1}$, 1I, 6M

Perform the following calculations:

$$\begin{aligned} I &= (r \cdot \tilde{m}_4)^{-1} \\ \frac{1}{m_4} &= r \cdot r^2 \cdot I \\ \frac{1}{r} &= \tilde{m}_4 \cdot I \\ s_0 &= \frac{1}{r} \cdot s'_0 \\ s_1 &= \frac{1}{r} \cdot s'_1 \end{aligned}$$

$l = l_3x^3 + l_2x^2 + l_1x + l_0$, 3M

$$\begin{aligned} l &= su_2 = (s_1x + s_0)(x^2 + u_{21}x + u_{20}) \\ &= s_1x^3 + (s_0 + u_{21}s_1)x^2 + (s_0u_{21} + s_1u_{20})x + s_0u_{20} \end{aligned}$$

By combining $\tilde{w}_0 = u_{20} \cdot s_0$ and $\tilde{w}_1 = u_{21} \cdot s_1$, we save one multiplication in calculating l_1 :

$$\begin{aligned} l_2 &= s_0 + \tilde{w}_1 \\ l_1 &= (s_0 + s_1) \cdot (u_{21} + u_{20}) - \tilde{w}_0 - \tilde{w}_1 \\ l_0 &= \tilde{w}_0 \end{aligned}$$

$m' = x^4 + m'_3x^3 + m'_2x^2 + \dots, u' = x^2 + u'_1x + u'_0$, 6M

We now make m monic by multiplying m_3 and m_2 by $\frac{1}{m_4}$:

$$\begin{aligned} m'_3 &= \left(\frac{1}{m_4}\right)(k_3 - s_1(l_2 + h_2) - s_0(l_3 + h_3)) \\ &= \left(\frac{1}{m_4}\right) \cdot (k_3 - s_1 \cdot (s_0 + l_2 + h_2) - h_3s_0) \\ m'_2 &= \left(\frac{1}{m_4}\right) \cdot (k_2 - s_1 \cdot (l_1 + h_1 + 2v_{21}) - s_0 \cdot (l_2 + h_2)) \end{aligned}$$

We reduce by one multiplication by plugging in $l_3 = s_1$ and factoring out s_1 , and recognizing the h_3 either equals 0 or 1.

Now $u' = \frac{m'}{u} = \frac{x^4 + m'_3x^3 + m'_2x^2 + \dots}{x^2 + u_{11}x + u_{10}}$. Once again, the division is exact by the Mumford representation.

$$\begin{aligned} u'_1 &= m'_3 - u_{11} \\ u'_0 &= m'_2 - u_{10} - u_{11} \cdot u'_1 \end{aligned}$$

$v' \equiv h - v_2 - l \pmod{u'}$, 3M

Note that this step can be skipped if one wishes to directly plug into baby step, which can take in any degree 3 polynomial and returns a reduced basis vector.

The adapted and reduced bases are essentially the same, except for the leading term

$$\begin{aligned} v' &= (h_3 - l_3)x^3 + (h_2 - l_2)x^2 + (h_1 - v_{21} - l_1)x + (h_0 - v_{20} - l_0) \\ &\equiv (h_2 - l_2 - u'_1(h_3 - l_3))x^2 + (h_1 - v_{21} - l_1 - u'_0(h_3 - l_3))x + (h_0 - v_{20} - l_0) \\ &\equiv (h_1 - v_{21} - l_1 - u'_0 \cdot (h_3 - l_3) - u'_1 \cdot (h_2 - l_2 - u'_1 \cdot (h_3 - l_3)))x \\ &\quad + (h_0 - v_{20} - l_0 - u'_0 \cdot (h_2 - l_2 - u'_1 \cdot (h_3 - l_3))) \pmod{u' = x^2 + u'_1x + u'_0} \end{aligned}$$

Then

$$\text{Adapted Basis: } v'_3 = h_3 - l_3$$

$$\text{Reduced Basis: } v'_3 = h_3 - l_3 - 2$$

$$v'_2 = h_2 - l_2 - u'_1 \cdot v'_3$$

$$v'_1 = h_1 - v_{21} - l_1 - u'_0 \cdot v'_3 - u'_1 \cdot v'_2$$

$$v'_0 = h_0 - v_{20} - l_0 - u'_0 \cdot v'_2$$

for a total of 4 multiplications. However, a more careful implementation removes one more multiplication:

$$\text{Adapted Basis: } v'_3 = h_3 - l_3$$

$$\text{Reduced Basis: } v'_3 = h_3 - l_3 - 2$$

$$\underline{w}_1 = u'_1 \cdot v'_3$$

$$v'_2 = h_2 - l_2 - \underline{w}_1$$

$$\underline{w}_0 = u'_0 \cdot v'_2$$

$$v'_1 = h_1 - v_{21} - l_1 - (u'_0 + u'_1) \cdot (v'_2 + v'_3) + \underline{w}_0 + \underline{w}_1$$

$$v'_0 = h_0 - v_{20} - l_0 - \underline{w}_0$$

This concludes the addition formulas.