Introduction to Cryptography: Assignment 11

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a) The point (19, 5) is on the curve, because:

$$\begin{aligned} y^2 &= x^3 + 11x + 18 \\ 5^2 &= 19^3 + 11 \cdot 19 + 18 \\ 25 &= 19^3 + 209 + 18 \\ 25 &= 6859 + 227 \\ 2 &\equiv 2 \pmod{23} \end{aligned}$$

The point (2,17) is not on the curve, because:

$$\begin{aligned} y^2 &= x^3 + 11x + 18 \\ 17^2 &\neq 2^3 + 11 \cdot 2 + 18 \\ 289 &\neq 8 + 22 + 18 \\ 289 &\neq 48 \\ 13 &\not\equiv 2 \pmod{23} \end{aligned}$$

(b) The points are (10, 1) and (10, 22) because:

$$\begin{aligned} y^2 &= x^3 + 11 \cdot x + 18 \\ y^2 &= 10^3 + 11 \cdot 10 + 18 \\ y^2 &= 1000 + 110 + 18 \\ y^2 &= 1128 \\ y^2 &\equiv 1 \pmod{23} \\ y &= \sqrt{1} \\ y = 1 \text{ or } y &= -1 \\ y \equiv 1 \text{ or } y &\equiv 22 \pmod{23} \end{aligned}$$

(c)

$$\begin{aligned}
R &= P + Q \\
\lambda &= \frac{y_p - y_q}{x_p - x_q} \\
\lambda &= \frac{4 - 8}{15 - 14} \\
\lambda &= \frac{-4}{1} \equiv 19 \pmod{23}
\end{aligned}$$

$$\begin{aligned}
x_r &= \lambda^2 - x_p - x_q \\
x_r &= 19^2 - 15 - 14 \\
x_r &\equiv 10 \pmod{23} \\
y_r &= \lambda(x_p - x_r) - y_p \\
y_r &= \lambda(15 - 10) - 4 \\
y_r &= 19 \cdot 5 - 4 \\
y_r &\equiv 22 \pmod{23}
\end{aligned}$$

Thus $R = P + Q = (10, 22)$. This is correct because:

$$\begin{aligned}
y^2 &= x^3 + 11 \cdot x + 18 \\
22^2 &= 10^3 + 11 \cdot 10 + 18 \\
1 &\equiv 1 \pmod{23}
\end{aligned}$$

(d)

$$\begin{aligned}
R &= P + P \\
a &= 11 \\
\lambda &= \frac{3x_p^2 + a}{2y_p} \\
\lambda &= \frac{3 \cdot 15^2 + 11}{2 \cdot 4} \\
\lambda &= \frac{19}{8} \pmod{23} \\
\lambda &= 19 \cdot 8^{-1} \pmod{23} \\
\lambda &= 19 \cdot 8^{\phi(23)-1} \pmod{23} \\
\lambda &\equiv 19 \cdot 8^{21} \equiv 19 \cdot 3 \pmod{23} \\
\lambda &\equiv 11 \pmod{23}
\end{aligned}$$

$$\begin{aligned}
x_r &= \lambda^2 - x_p - x_p \\
x_r &= 11^2 - 15 - 15 \\
x_r &\equiv 22 \pmod{23} \\
y_r &= \lambda(x_p - x_r) - y_p \\
y_r &= \lambda(15 - 22) - 4 \\
y_r &= 11 \cdot -7 - 4 \\
y_r &\equiv 11 \pmod{23}
\end{aligned}$$

Thus $R = P + P = (22, 11)$. This is correct because:

$$\begin{aligned} y^2 &= x^3 + 11 \cdot x + 18 \\ 11^2 &= 22^3 + 11 \cdot 22 + 18 \\ 6 &\equiv 6 \pmod{23} \end{aligned}$$

(e) The order of the elliptic curve is 31. This is a prime number, which means that the order of all generators is also 31 (Lagrange). So we can choose any point on the curve as a generator, for example (7, 1). This point is on the curve because: $y^2 = 7^3 + 11 \cdot 7 + 18 = 1 \pmod{23}$.

(f) For every $y \mod 23$ that is even, $-y \mod 23$ will be odd because 23 is odd. E.g. $y = 4$, then $-y = -4 \mod 23 = 19$.

(g) If a point has an order of 2, then $P = x \cdot P$ with x as a positive odd number. If x is a positive even number then $x \cdot P = \mathcal{O}$.

(h) No, because $\#\mathcal{E}(\mathbb{F}_{23}) = 31$, which is a prime number and according to Lagrange, this means that all the elements in this group have an order that can be divided by said prime number.

(i) $y^2 = 20^3 + 11 \cdot 20 + 18 = 4 \pmod{23}$
$y = \sqrt{4}$
$y = 2$ or $y = -2$
$y \equiv 2$ or $y \equiv 21 \pmod{23}$
So $T = (20, 21)$ because $T_y^c = 1$ (odd).

2

(a)

$$\begin{aligned} y^2 &= x^3 + 12x + 15 \\ 3^2 &= 3^3 + 3 \cdot 12 + 15 \\ 9 &= 27 + 36 + 15 \\ 9 &= 9 \pmod{23} \end{aligned}$$

(b)

$$\begin{aligned} &R = Q + Q \\ &a = 12 \\ &\lambda = \frac{3x_q^2 + a}{2y_q} \\ &\lambda = \frac{3 \cdot 3^2 + 12}{2 \cdot 3} \\ &\lambda = \frac{16}{6} \pmod{23} \\ &\lambda = 16 \cdot 6^{-1} \pmod{23} \\ &\lambda = 16 \cdot 6^{\phi(23)-1} \pmod{23} \\ &\lambda \equiv 16 \cdot 6^{21} \equiv 16 \cdot 4 \pmod{23} \\ &\lambda \equiv 18 \pmod{23} \end{aligned}$$

$$\begin{aligned}
x_r &= \lambda^2 - x_q - x_q \\
x_r &= 18^2 - 3 - 3 \\
x_r &\equiv 19 \pmod{23} \\
y_r &= \lambda(x_q - x_r) - y_q \\
y_r &= \lambda(3 - 19) - 3 \\
y_r &= 18 \cdot -16 - 3 \\
y_r &\equiv 8 \pmod{23}
\end{aligned}$$

Thus $R = Q + Q = (19, 8)$. This is correct because:

$$\begin{aligned}
y^2 &= 19^3 + 12 \cdot x + 15 \\
8^2 &= 19^3 + 12 \cdot 19 + 15 \\
18 &\equiv 18 \pmod{23}
\end{aligned}$$

(c) Lagrange's theorem: The order of every point on the curve divides the order of the curve. The order of the curve is 33, so the possible orders of the points are any number that can divide 33 into a whole number (1, 3, 11, 33).

(d)

$$\begin{aligned}
Q &= (3, 3) \\
[2]Q &= (19, 8) \longleftarrow \text{See 2.b} \\
[3]Q &= [2]Q + Q = \\
\lambda &= \frac{y_{[2]q} - y_q}{x_{[2]q} - x_q} \\
\lambda &= \frac{8 - 3}{19 - 3} \\
\lambda &= \frac{5}{16} \equiv 19 \pmod{23} \\
\lambda &= 5 \cdot 16^{-1} \pmod{23} \\
\lambda &= 5 \cdot 16^{\phi(23)-1} \pmod{23} \\
\lambda &\equiv 5 \cdot 16^{21} \equiv 5 \cdot 13 \pmod{23} \\
\lambda &\equiv 19 \pmod{23} \\
x_{[3]q} &= \lambda^2 - x_{[2]q} - x_q \\
x_{[3]q} &= 19^2 - 19 - 3 \pmod{23} \\
x_{[3]q} &\equiv 17 \pmod{23} \\
y_{[3]q} &= \lambda(x_{[2]q} - x_{[3]q}) - y_{[2]q} \\
y_{[3]q} &= \lambda(19 - 17) - 8 \\
y_{[3]q} &= 19 \cdot 2 - 8 \\
y_{[3]q} &\equiv 7 \pmod{23}
\end{aligned}$$

This means that the order of $(3, 3) \neq 3$ and because the order is not 33 as stated in the assignment, this means that ord$(3, 3) = 11$ as that is the only possible order left.

(e) $Z = 1$
$X = x * Z = 3 \cdot 1 = 3$
$Y = y * Z = 3 \cdot 1 = 3$
So $(3 : 3 : 1)$ are the protective coordinates for the point Q.

(f) $Z^{-1} = 4^{\phi(23)-1} = 4^{21} = 6 \pmod{23}$ The affine representation is $(X \times Z^{-1}, Y \times Z^{-1}) = (9 \times 6, 20 \times 6) = (8, 5)$.

3

(a) $A \longleftarrow [a]G$ with $a = 3$

$$\begin{aligned}
G &= (1,7)\\
a &= 5\\
[2]G &= G + G\\
\lambda &= \frac{3x_g^2 + a}{2y_g}\\
\lambda &= \frac{3 \cdot 1^2 + 5}{2 \cdot 7}\\
\lambda &= \frac{8}{14}\\
\lambda &= 8 \cdot 14^{-1}\\
\lambda &= 8 \cdot 14^{\phi(13)-1}\\
\lambda &= 8 \cdot 14^{11}\\
\lambda &\equiv 8 \cdot 1 \pmod{13}\\
\lambda &\equiv 8 \pmod{13}\\
x_{[2]g} &= \lambda^2 - x_g - x_g\\
x_{[2]g} &= 8^2 - 1 - 1 \pmod{13}\\
x_{[2]g} &\equiv 10 \pmod{13}\\
y_{[2]g} &= \lambda(x_g - x_{[2]g}) - y_g\\
y_{[2]g} &= 8 \cdot (1 - 10) - 7\\
y_{[2]g} &= 8 \cdot -9 - 7\\
y_{[2]g} &\equiv 12 \pmod{13}
\end{aligned}$$

$$
\begin{aligned}
G &= (1,7) \\
[2]G &= (10,12) \\
[3]G &= [2]G + G \\
\lambda &= \frac{y_{[2]g} - y_g}{x_{[2]g} - x_g} \\
\lambda &= \frac{12-7}{10-1} \\
\lambda &= \frac{5}{9} \\
\lambda &= 5 \cdot 9^{-1} \\
\lambda &= 5 \cdot 9^{\phi(13)-1} \\
\lambda &= 5 \cdot 9^{11} \equiv 5 \cdot 3 \pmod{13} \\
\lambda &\equiv 2 \pmod{13} \\
x_{[3]g} &= \lambda^2 - x_{[2]g} - x_g \\
x_{[3]g} &= 2^2 - 10 - 1 \\
x_{[3]g} &\equiv 6 \pmod{13} \\
y_{[3]g} &= \lambda(x_{[2]g} - x_{[3]g}) - y_{[2]g} \\
y_{[3]g} &= \lambda(10-6) - 12 \\
y_{[3]g} &= 2 \cdot 4 - 12 \\
y_{[3]g} &\equiv 9 \pmod{13}
\end{aligned}
$$

So Alice's public key is $[3]G = (6,9)$.

(b) The compressed point representation is $(6,1)$, because $9 \mod 2 = 1$.

(c) $y^2 = 4^3 + 5 \cdot 4 + 4 = 10 \pmod{13}$
$y = \sqrt{10}$
$y = 6$ or $y = -6$
$y \equiv 6$ or $y \equiv 7 \pmod{13}$
So Bob's public key is $(4,7)$.

(d) The shared key of Alice and Bob is $[a]B$: $P \longleftarrow [a]B$ with $a = 3$

$$
\begin{aligned}
B &= (4,7) \\
a &= 5 \\
[2]B &= B + B \\
\lambda &= \frac{3x_b^2 + a}{2y_b} \\
\lambda &= \frac{3 \cdot 4^2 + 5}{2 \cdot 7} \\
\lambda &= \frac{53}{14} \\
\lambda &= 53 \cdot 14^{-1} \\
\lambda &= 53 \cdot 14^{\phi(13)-1} \\
\lambda &= 53 \cdot 14^{11} \\
\lambda &\equiv 53 \cdot 1 \pmod{13} \\
\lambda &\equiv 1 \pmod{13} \\
x_{[2]b} &= \lambda^2 - x_b - x_b \\
x_{[2]b} &= 1^2 - 4 - 4 \pmod{13} \\
x_{[2]b} &\equiv 6 \pmod{13} \\
y_{[2]b} &= \lambda(x_b - x_{[2]b}) - y_b \\
y_{[2]b} &= 1 \cdot (4 - 6) - 7 \\
y_{[2]b} &= -2 - 7 \\
y_{[2]b} &\equiv 4 \pmod{13}
\end{aligned}
$$

$$
\begin{aligned}
[2]B &= (6,4) \\
[3]B &= [2]B + B \\
\lambda &= \frac{y_{[2]b} - y_b}{x_{[2]b} - x_b} \\
\lambda &= \frac{4 - 7}{6 - 4} \\
\lambda &= \frac{-3}{2} \\
\lambda &= -3 \cdot 2^{-1} \\
\lambda &= -3 \cdot 2^{\phi(13)-1} \\
\lambda &= -3 \cdot 2^{11} \equiv 10 \cdot 7 \pmod{13} \\
\lambda &\equiv 5 \pmod{13} \\
x_{[3]b} &= \lambda^2 - x_{[2]b} - x_b \\
x_{[3]b} &= 5^2 - 6 - 4 \\
x_{[3]b} &\equiv 2 \pmod{13} \\
y_{[3]b} &= \lambda(x_{[2]b} - x_{[3]b}) - y_{[2]b} \\
y_{[3]b} &= \lambda(6 - 2) - 4 \\
y_{[3]b} &= 5 \cdot 4 - 4 \\
y_{[3]b} &\equiv 3 \pmod{13}
\end{aligned}
$$

The shared secret point P is thus $(2,3)$.