Elliptic Curve Cryptography

1. a) $\Delta \equiv 12 \bmod 19$. Since $9^2 = 4^3 + 3 \cdot 4 + 5$, the point $P = (4, 9)$ lies on the curve. We use the formulas for point addition. The slope is $m = 6$ and $2 \cdot P = (9, 18)$.
   b) $\Delta = -12528$, $P = (4, 9) \in E(\mathbb{Q})$, $m = \frac{17}{6}$ and $2 \cdot P = (\frac{1}{36}, \frac{487}{216})$.
2. a) Hasse's Theorem implies $|23 + 1 - \mathrm{ord}\,(E(GF(23)))| \leq 9.59$ and hence
   $$15 \leq \mathrm{ord}\,(E(GF(23))) \leq 33.$$
   b) Since the order of $E(GF(23))$ is less than or equal to 33, five point doublings and five additions are sufficient when using the double-and-add algorithm, i.e., at most 10 point operations. In fact, 9 point operations are sufficient.
3. Let $(x, y) \in E_{ns}(K)$ be an affine point and $f(x, y) = \frac{x}{y} = t$. The map is well-defined, since $y = 0$ implies $x = 0$. But $(0, 0)$ is a singular point. Since $y^2 = x^3$, we have $(\frac{y}{x})^2 = x$ and $(\frac{y}{x})^3 = y$. Hence $x = (\frac{1}{t})^2$ and $y = (\frac{1}{t})^3$. This shows that x and y are uniquely determined by t. For any $t \in K^*$, the associated values for x and y satisfy the equation $y^2 = x^3$. It follows that f is a bijection between the affine points of $E_{ns}(K)$ and K^*. The point at infinity is mapped to 0, and so we get a bijection between $E_{ns}(K)$ and K.

   Now let (x_1, y_1), $(x_2, y_2) \in E_{ns}(K)$ be two affine points and suppose the sum of these two points using the addition law on elliptic curves is (x_3, y_3). Set $t_i = \frac{x_i}{y_i}$ for $i = 1, 2, 3$. We claim that $t_1 + t_2 = t_3$, which would prove that f is a homomorphism. Suppose $x_1 \neq x_2$; then we have $m = \frac{y_2 - y_1}{x_2 - x_1}$ and
   $$t_3^{-2} = x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 = \left(\frac{t_2^{-3} - t_1^{-3}}{t_2^{-2} - t_1^{-2}}\right)^2 - t_1^{-2} - t_2^{-2}.$$
   A straightforward computation gives $t_3^{-2} = (t_1 + t_2)^{-2}$. Let's look at the y-coordinate:
   $$t_3^{-3} = y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 = \frac{t_2^{-3} - t_1^{-3}}{t_2^{-2} - t_1^{-2}}(t_1^{-2} - t_3^{-2}) - t_1^{-3}$$
   This can be rearranged to $t_3^{-3} = (t_1 + t_2)^{-3}$. Finally, we obtain
   $$t_3 = \frac{t_3^{-2}}{t_3^{-3}} = \frac{(t_1 + t_2)^{-2}}{(t_1 + t_2)^{-3}} = t_1 + t_2.$$
   Now suppose that $x_1 = x_2$. Then $m = \frac{3x_1^2}{2y_1} = \frac{3}{2}t_1^{-1}$ and
   $$t_3^{-2} = x_3 = m^2 - 2x_1 = \frac{9}{4}t_1^{-2} - 2t_1^{-2} = \frac{1}{4}t_1^{-2}.$$
   Furthermore, the y-coordinate is
   $$t_3^{-3} = y_3 = m(x_1 - x_3) - y_1 = \frac{3}{2}t_1^{-1}\left(t_1^{-2} - \frac{1}{4}t_1^{-2}\right) - t_1^{-3} = \frac{1}{8}t_1^{-3}.$$
   This implies
   $$t_3 = \frac{t_3^{-2}}{t_3^{-3}} = 2t_1.$$
4. First, we verify that p and n are prime numbers:

```
sage: p=0xA9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
sage: p.is_prime()
True
sage: n=0xA9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
sage: n.is_prime()
True
```

The parameters define a nonsingular curve E over $GF(p)$:

```
sage: a = 0x7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
sage: b = 0x26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
sage: disc=-16*(4*a^3+27*b^2);mod(disc,p)
15036242490247342171513009477805930598983339216081386851174014206346325949410
sage: E=EllipticCurve(GF(p),[a,b])
```

We verify that the order of $E(GF(p))$ is n. The computation of the order may take a few seconds.

```
sage: E.order()==n
True
```

Then we check that $g = (x_g, y_g) \in E(GF(p))$:

```
sage: xg=0x8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262
sage: yg=0x547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
sage: g=E(xg,yg)
```

Since $E(GF(p))$ has prime order n, the order of the nonzero point g must be n. Finally, we check that $\operatorname{ord}(p \bmod n)$ is large:

```
sage: mod(p,n).multiplicative_order()
38442478198522672110404873314500824546368765892207264769377759531531768179539
```

In fact, we have $\operatorname{ord}(p \bmod n) = \frac{n-1}{2}$.

5. Use SageMath.
   $A =$
   $(30786306364684019669845085647834227301026705121148702657850323422577469426661,$
   $62738119601096463087058618165599972860801258532835385944058084661017583328220)$.
   $B =$
   $(63856341335644447573330799294730313060965602021945406582077408231386506305403,$
   $69225670661515104449943687281706110118505391815211949231460931578788174425194)$.
   $b \cdot A = a \cdot B = k =$
   $(62277408572425350581153587818274169049667602786711788049878422423086378303275,$
   $33362437316335065570684137232427223851259119247580365682976721759161769329886)$.
6. a) Define an elliptic curve E over $\mathbb{Z}_N$ and a point $P \in E(\mathbb{Z}_N)$.
   Since $\gcd(\Delta, N) = 1$, the curve is nonsingular over $\mathbb{Z}_N$.

```
sage: N=6227327; a=4;u=6;v=2;b=v^2-u^3-a*u
sage: disc=-16*(4*a^3+27*b^2);gcd(disc,N)
1
sage: E=EllipticCurve(IntegerModRing(N),[a,b])
sage: P=E(u,v)
```

b) $Q = (12!)P$ is an affine point. However, $(13!)P = 13Q$ does not give an affine point of E over $\mathbb{Z}_N$. In fact, $12Q$ exists, but the addition $12Q + Q = 13Q$ does not work.

```
sage: Q=factorial(12)*P;Q
 (3183142 : 5717628 : 1)
sage: factorial(13)*P
(Error)
sage: 12*Q
(506293 : 4862299 : 1)
```

c) The critical denominator used in the computation of $12Q+Q$ is the difference of the x-coordinates of $12Q$ and Q. The gcd of that difference and N gives the factor $p = 3109 \mid N$.

```
sage: gcd(3183142-506293,N)
3109
```

d) The second factor is $q = \frac{N}{p} = 2003$. We explain why the method was successful. To this end, we compute the order of P in $E(GF(p))$ and $E(GF(q))$.

```
sage: p=3109;q=2003
sage: Ep=EllipticCurve(GF(p),[a,b])
sage: P=Ep(u,v)
sage: P.order().factor()
 2^3 * 3 * 5 * 13
sage: Eq=EllipticCurve(GF(q),[a,b])
sage: P=Eq(u,v)
sage: P.order().factor()
7 * 17^2
```

We see that $(13!)P = O \bmod p$, but $(13!)P \neq O \bmod q$.

7. a) Let r be the x-coordinate modulo n of the point $k \cdot g$ and

$$s = k^{-1}(H(m) + ar) \bmod n.$$

The signature parameters r and s must be nonzero.
Then $k = s^{-1}(H(m) + ar) \bmod n$ and

$$R = s^{-1}H(m) \cdot g + s^{-1}r \cdot A = s^{-1}(H(m) + ar) \cdot g = k \cdot g.$$

We have shown that $R = k \cdot g$, and so the x-coordinate of R modulo n is r.
b) We compute $A = a \cdot g = (11, 18)$ and $k \cdot g = (9, 1)$. The x-coordinate of $k \cdot g$ modulo 13 is $r = 9$. Furthermore, $k^{-1} = (3 \bmod 13)^{-1} \equiv 9$. Then $s = 9 \cdot (11 + 2 \cdot 9) \equiv 1 \bmod 13$ and the signature is $(r, s) = (9, 1)$.
To verify the signature, we check that r and s lies between 1 and 12. Then we compute

$$R = s^{-1}H(m) \cdot g + s^{-1}r \cdot A = 11 \cdot (18, 18) + 9 \cdot (11, 18) = (9, 1).$$

The x-coordinate of R modulo 13 is 9, which is equal to r. This verifies the signature.
c) If a signature (r, s), a hash $H(m)$, the order n and k is known, then an adversary can compute $s\,k = H(m) + ar \bmod n$ and thus obtain the secret key:

$$a = r^{-1}(s\,k - H(m)) \bmod n$$